VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV MIKROELEKTRONIKY

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF MICROELECTRONICS

JIŠTĚNÝ ŘÍDICÍ SYSTÉM

SECURED CONTROL SYSTEM

DIPLOMOVÁ PRÁCE
MASTER´S THESIS

AUTOR PRÁCE — Bc. MICHAL KUBÁŇ
AUTHOR

VEDOUCÍ PRÁCE — Ing. MICHAL PAVLÍK, Ph.D.
SUPERVISOR

BRNO 2010

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav mikroelektroniky

Diplomová práce

magisterský navazující studijní obor
Mikroelektronika

Student:	Bc. Michal Kubáň	***ID:***	83566
Ročník:	2	***Akademický rok:***	2009/2010

NÁZEV TÉMATU:

Jištěný řídicí systém

POKYNY PRO VYPRACOVÁNÍ:

Navrhněte a zrealizujte terciálně jištěný řídicí systém malé vodní elektrárny (dále jen MVE). Při návrhu zohledněte specifika potřeby nepřetržitého řízení MVE. Řídicí systém MVE musí být schopen obsluhovat 1 až 10 vodních turbín a elektrické čištění česlí vtoku do MVE. Obsluha turbíny zahrnuje kontrolu, jestli jsou splněny podmínky pro bezpečný provoz turbíny a samotnou regulaci turbíny podle stavu vody na toku, kde je MVE instalována.

DOPORUČENÁ LITERATURA:

Dle pokynu vedoucího práce

Termín zadání:	8.2.2010	***Termín odevzdání:***	27.5.2010

Vedoucí práce: Ing. Michal Pavlík, Ph.D.

prof. Ing. Vladislav Musil, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Místo pro lic. Smlouvu

Poděkování

Tímto děkuji mému vedoucímu Ing. Michalu Pavlíkovi, Ph.D., za trpělivé vedení a přínosné rady během celé práce. Dále Ing. Alešovi Marvanovi za podnětné rady a pomoc při praktické realizaci. Celá práce by nevznikla bez vytrvalé podpory mojí rodiny, slečny i přátel, děkuji vám. Největší dík však patří Bohu.

Abstrakt

Tato práce pojednává o konstrukci jištěného řídicího systému malé vodní elektrárny (dále jen MVE). Jištěný řídicí systém spadá pod systémy odolné proti poruchám (angl. Fault Tolerant Systems). Nejdříve jsou rozebrány požadavky kladené na řídicí systém MVE. Práce se dále zabývá úvodem do problematiky systémů odolných proti poruchám. Požadavky na řídicí systém MVE a základy systémů odolných proti poruchám, jsou použity jako výchozí podklady ke specifikaci jištěného řídicího systému, jenž je v rámci této práce realizován.

Abstract

This work deals with the design of a small hydro secured control system. The secured control system itself belongs to the Fault Tolerant Systems category. At first the requirements on small hydro control system are discussed. Then the introduction into the basics of Fault Tolerant System theory is given. The requirements on small hydro control system and basics of Fault Tolerant Systems are basis for specification of secured control system which design and construction is the main objective of this work.

Obsah

1. Úvod

Předmětem této práce je návrh jištěného řídicího systému, demonstrovaný na řídicím systému malé vodní elektrárny (dále jen MVE).

Pro návrh takového systému je nutné:

- Seznámit se s požadavky kladenými na řídicí systém MVE.
- Osvojit si základy problematiky jištěných řídicích systémů.
- Navrhnout řídicí systém splňující požadavky kladené na řídicí systém MVE.
- Vypracovat případové studie nejzávažnějších a nejvíce pravděpodobných poruch řídicího systému MVE.
- Pomocí poznatků z teorie jištěných systémů zodolnit navržený řídicí systém proti poruchám, které jsou výsledkem případových studií.

Na základě získaných poznatků je možné přistoupit k vlastnímu návrhu jištěného řídicího systému MVE.

1.1 Vodní turbína

Informace o prvopočátcích využívání energie vody (potenciální a z ní plynoucí kinetické) nejsou úplně jednoznačné. Některé prameny hovoří o využívání lžícového vodního kola Egypťany k pohonu věder na čerpání vody již roku 230 př. Kr. [Elek2]. Jiné zdroje uvádí, že se ve 2. století př. Kr. v Ilyrii (západní část Balkánského poloostrova) využívaly k pohonu mlýnských kamenů vodní kola s vertikální hřídelí [Elek0].

Co však z výše uvedeného jasně plyne je, že lidé využívají vodní energii už více než 2 000 let. Samozřejmě stroje, které zprostředkovávají přeměnu vodní kinetické energie na jinou energii, se za tu dobu značně změnily. Dnešní turbíny byly vyvinuty na základě lopatkových strojů zásluhou Jána Andreje Segnera (1704 – 1783), původem z Bratislavy, později profesora Univerzity v Göttingen [Elek0, Elek3]. Segnerovo kolo, které vymyslel, se používalo jako vodní motor.

Po roce 1750 propracovali Leonard Euler (švýcarského původu, 1707-1783) a Daniel Bernoulli (holandského původu, 1700-1782) teorii dynamiky ideální kapaliny. Stalo se tak v Petrohradě, kde působili jako členové Ruské akademie věd a znamenalo to položení teoretického základu pro stavbu hydraulických strojů, tedy dnešních vodních turbín a čerpadel [Elek3].

První vodní turbíny vyvinuli pánové Bourdin a Fourneyron v 19. st. (oba francouzského původu). Fourneyron v postatě zdokonalil Bourdinův první pokus o vodní turbínu a zkonstruoval první odstředivou turbínu. Pracovala od r. 1835 do r. 1865 a byla určena pro spád H = 108 m, průtok Q = 35 l/s. Měla otáčky n = 2300 min^{-1} a výkon P = 40 k.

Následovaly turbíny pro střední a vysoké spády – J. B. Francis r. 1849 a L. A. Pelton r. 1880 (oba amerického původu) [Elek3]. Jednodušší alternativou Francisovy turbíny je Bánkiho turbína. Teoreticky ji vynalezl australský inženýr A. G. M. Mitchel r. 1903, pro praktické použití ji r. 1918 dopracoval maďarský profesor D. Banki [Elek7].

Roku 1919 patentoval Victor Kaplan, profesor na tehdejší německé vysoké škole technické v Brně, axiální přetlakovou turbínu pro nízké spády a větší průtoky [Elek3].

Zjednodušeně lze říci, že na malé průtoky a malé spády je vhodná Bánkiho turbína, na menší až střední spády s větším průtokem jsou vhodné Francisovy turbíny a na menší až střední spády s velkým průtokem je vhodná Kaplanova turbína [Elek4].

1.2 Malá vodní elektrárna, MVE

První malé vodní elektrárny byly budovány počínaje rokem 1881 v USA a Anglii. Byly využívány jako zdroje pro osvětlení [Elek0].

V současné době je termín MVE používán k označení vodní elektrárny s instalovaným výkonem (tj. celkovým výkonem generátorů elektrické energie poháněných turbínami) do 10 MW [Elek1]. Evropská unie však jako malou vodní elektrárnu chápe vodní elektrárnu s instalovaným výkonem jen do 5 MW [Wiki2].

Některé zdroje uvádí podrobnější dělení MVE [Elek8]:

- Průmyslové (od 1 MW do 10 MW).
- Závodní, nebo veřejné (od 0,1 MW do 1 MW).
- Drobné elektrárny, mini-elektrárny (od 0,035 MW do 0,1 MW).
- Mikrozdroje, mobilní zdroje (do 0,035 MW).

V České Republice je situace s malými vodními elektrárnami přibližně následující [Wiki1]:

- Je zde nejméně 54 MVE.
- Z nich 27 má instalovaný výkon 1 MW a více.
- Naproti tomu 27 má instalovaný výkon do 1 MW, z toho 8 má instalovaný výkon do 0,1 MW včetně.

MVE s instalovaným výkonem přesahujícím 1 MW často vlastní stát, nebo velké společnosti. Mnohé MVE s výkonem do 0,1 MW jsou v soukromém vlastnictví a informace o nich proto nejsou k dispozici. Malých elektráren je mnohem víc než zde uvedených 8, poněvadž seznam postihuje převážně elektrárny většího významu a není proto zdaleka vyčerpávající.

1.3 Popis MVE

MVE se typicky realizují jako [Elek3]:

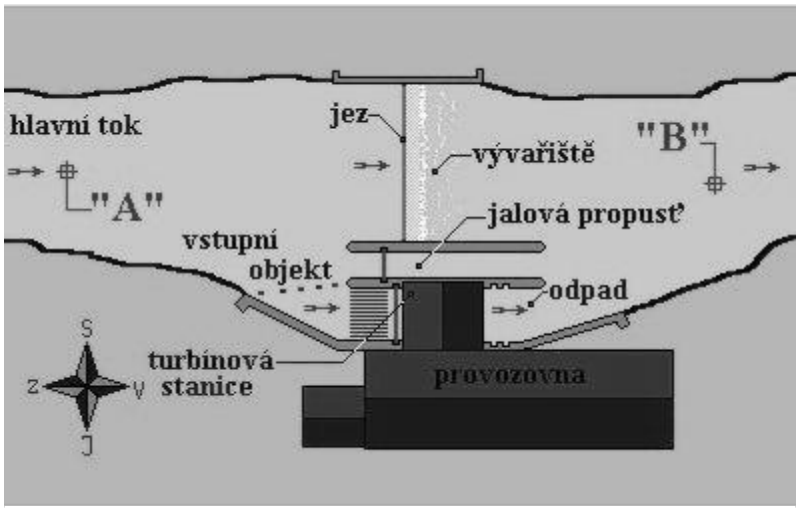
- Říční systémy (jezové, přehradové).
- Derivační systémy.
- Akumulační systémy.

1.3.1 Říční systémy MVE

Jsou charakteristické tím, že MVE je součástí vzdouvacího objektu, a to jezu nebo přehrady.

Jezové MVE (obr. 2) buď leží v blízkosti jezu na přilehlém kanále, nebo jsou přímo součástí jezového tělesa, takže voda přiváděná do turbíny v podstatě neopouští koryto řeky [Elek3].

Oblíbenou možností, jak zvýšit spád na již hotovém jezu, je použití tzv. vakového jezu. Jedná se o pryžový válec ukotvený před korunou jezu. Zabírá celou šířku toku řeky a vzdutí se dosahuje napuštěním vakového jezu vodou. Množstvím vody ve vakovém jezu lze regulovat velikost vzdutí. V případě povodně lze vakový jez úplně vypustit. Potom má jez stejnou výšku jako před instalací vakového jezu.



Obr. 1 Jezová MVE [ObrElek1]

Komplikovanější alternativou k vakovému jezu jsou kovové klapky, taktéž ukotvené před korunou jezu a ovládané hydraulickými pístnicemi. Princip činnosti je podobný, jako u vakového jezu. Velikost vzdutí se reguluje sklonem klapek. Jsou-li klapky ve svislé poloze, je vzdutí největší. Pokud jsou ve vodorovné poloze má jez svůj původní spád.

Výhodou klapek oproti vakovému jezu je jejich větší robustnost, vakový jez může být např. prořezán. Vakový jez lze nicméně realizovat z různě silné a mohutné pryže. Je-li z masivní pryže, dokáže naopak díky své pružnosti snáze odolávat nárazům kusů dřeva a kamenů unášených velkou vodou. Ty by mohly klapky svým nárazem zdeformovat. Navíc u vakového jezu odpadají klouby, které je potřeba mazat ekologickým tukem. Vakový jez nevyžaduje ani hydraulické pístnice, které je také potřeba provozovat s ekologicky odbouratelným olejem a kontrolovat jejich těsnost. Vlhké prostředí je navíc pro pístnice agresivní a zkracuje jejich životnost.

Přehradové MVE mají vlastní strojovnu umístěnou částečně nebo úplně v tělese přehrady. Přívod k turbínám je řešen krátkým přivaděčem a odpad (tvořený sací troubou) ústí přímo do spodního objektu nebo dolní nádrže. Voda, která se nevyužije v turbínách, přepadá přes jezová pole či přepady v hrázi přehrady [Elek3].

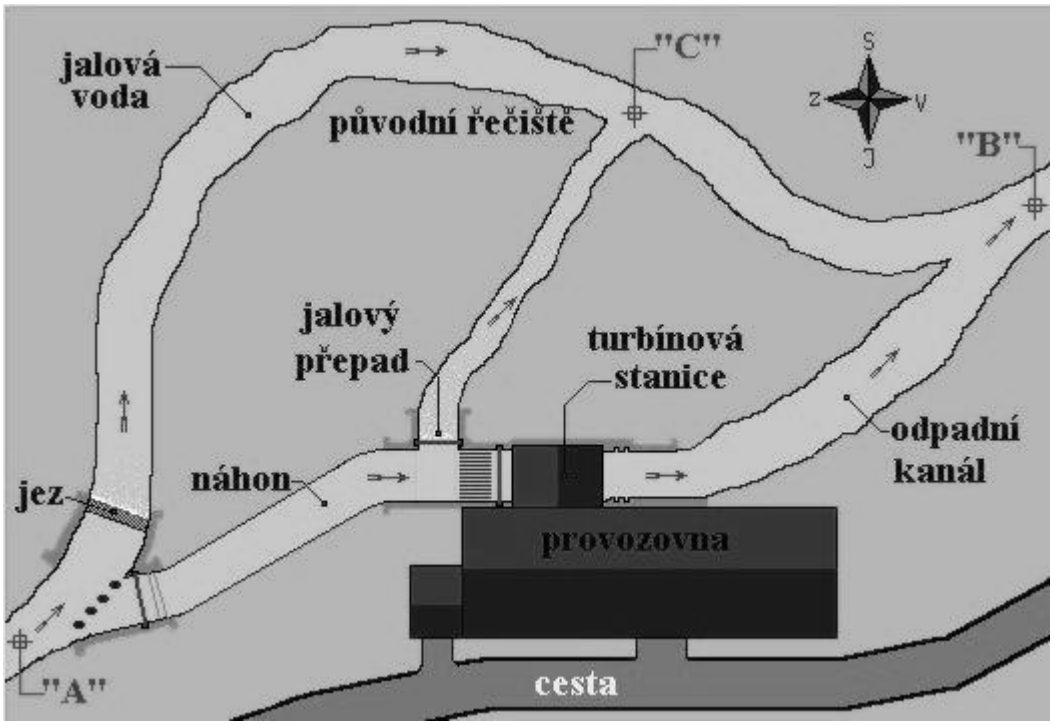
Ve většině případů se jedná o vodní díla s nízkým nebo se středním spádem, kde jsou použity turbíny Kaplanovy (různých modifikací) nebo

turbíny Francisovy. U jezových MVE se jedná o spády do H=20m a u přehradových jsou to střední spády do H=70m.

1.3.2 Derivační systémy MVE

Derivační systémy mohou být pro nízké spády řešeny jako kanálové (s volnou hladinou až k turbínám), nebo pro střední a vysoké spády s derivačním tlakovým přivaděčem.

Tyto MVE zkracují délku řečiště mezi místy A-B (obr. 2), mezi kterými se soustřeďuje využitelný spád. Derivační kanál (většinou betonový) má menší hydraulické ztráty než původní řečiště, přičemž umožňuje navíc rovnoměrnou změnu rychlosti proudění před vtokem do turbín. Vzdouvacím zařízením takového systému může být jez nebo přehrada. Vtokový objekt obsahuje hrubé česle, stavidla a usazovací nádrž s proplachovacím kanálem. Objekt vlastní MVE je tvořen strojovnou s vodní turbínou, generátorem a příslušenstvím. Na vtoku jsou instalovány jemné česle a přepad, pro zajištění tzv. asanačního průtoku. Na výtoku je jalová výpusť a spodní kanál [Elek3].



Obr. 2 Derivační systém MVE [ObrElek2]

Při vyšších spádech (nad H=50÷70m) nelze vodu přivádět otevřeným kanálem až k turbínám, proto se voda z HN vede tlakovým přivaděčem (např. betonovou štolou nebo ocelovým potrubím) přímo do vstupního profilu turbín.

Derivační systémy zahrnují MVE s malými, středními i vyššími spády, ve kterých jsou instalovány různé druhy vodních turbín, např. turbíny Kaplanovy různých modifikací, diagonální-Dériazovy, Francisovy i Peltonovy turbíny [Elek3].

1.3.3 Akumulační systémy špičkových MVE

V případě vhodných geologických podmínek je možné řešit MVE jako špičkovou, nebo z jiného úhlu pohledu, jako MVE s možností akumulace hydraulické energie v horní nádrži. Jde tedy o MVE přehradové, avšak s přehradou, která je schopna po určitou dobu zásobovat turbíny větším průtokem, než jaký poskytuje přítok řekou. To je výhodné např. v době velké spotřeby, tzv. špičkového zatížení. Popsaná MVE spadá do kategorie s tzv. primární, nebo přirozenou akumulací.

Mezi akumulační systémy patří i přečerpávací vodní elektrárny. Jde o elektrárny s tzv. sekundární akumulací, kdy se voda v době přebytku elektrické energie, čerpá z dolní nádrže do horní nádrže. Přečerpávací elektrárny se však nejčastěji budují za účelem pokrytí špičkového odběru celostátní rozvodné sítě a proto svým výkonem mnohonásobně překračují výkon MVE [Elek3].

1.3.4 Generátory pro MVE

V zásadě se generátory dělí na dva druhy:

- Synchronní
- Asynchronní

Synchronní generátor, neboli také alternátor, ke své činnosti nepotřebuje trojfázové budící napětí a proud. Místo toho se budí stejnosměrným napětím a proudem. To se přivádí do vinutí na rotoru. Velikost budícího napětí reguluje velikost vyráběného trojfázového napětí. Na velikost vyráběného napětí mají vliv také otáčky rotoru generátoru. Regulace výstupního napětí otáčkami rotoru se však nepoužívá, neboť změna otáček je jediný způsob, jak regulovat frekvenci vyráběného napětí – samozřejmě pokud nepočítáme změnu počtu pólů, což by však znamenalo použít jiný generátor, neboť počet pólů je jedním z konstrukčních parametrů generátoru. Stejnosměrné budící napětí se získává usměrněním síťového napětí, nebo jej lze generovat dynamem s paralelním buzením.

Existují i synchronní generátory s vestavěným usměrněným třífázovým budícím generátorem. Je nutné dát pozor na to, že díky zbytkovému (tzv. remanentnímu) magnetismu rotoru vyrábějí synchronní generátory napětí i pokud nejsou buzeny [Elek5]. Proto je velice důležité v případě výpadku napětí rozvodné elektrické sítě zajistit jejich odpojení. Výpadek napětí v rozvodné síti totiž může např. znamenat, že byl daný úsek sítě odpojen za účelem práce na vedení, nebo kvůli pracím na zařízení připojenému k vedení. Pokud by nebyl synchronní generátor včas odpojen, mohl by jím vyráběný elektrický proud ohrožovat životy pracovníků.

Synchronní generátor může pracovat i v tzv. ostrovní síti, kde je jediným zdrojem elektrické energie. Aby generoval elektrickou energii o správném napětí a frekvenci, je potřeba ho regulovat. Pokud je naopak připojen do veřejné rozvodné sítě, je nutné jej se sítí tzv. sfázovat. Znamená to zajistit shodné pořadí fází, napětí a frekvenci výstupu generátoru vzhledem k rozvodné síti. Sfázování se provádí při připojování generátoru k rozvodné

síti. Dříve se tento krok prováděl manuálně, avšak dnes je celý proces zautomatizován pomocí tzv. synchroskopů [Elek6].

Asynchronní generátor ke své činnosti potřebuje trojfázové budící napětí a proud, aby začal dodávat elektrickou energii zpět do rozvodné sítě. Jde vlastně o elektrický motor, který je turbínou nucen k otáčkám větším, než jsou jeho nominální otáčky. Místo odběru elektrické energie z rozvodné sítě, ji začne do sítě dodávat. Jakmile budící napětí vypadne, generátor přestane vyrábět elektrickou energii a začne se točit naprázdno. Nehrozí tedy nebezpečí, že by generátor dodával elektrickou energii do jinak úmyslně odpojené části elektrického vedení. Hrozí zde však jiné riziko. Přestane-li asynchronní generátor vyrábět elektrickou energii, začne se točit naprázdno. To ohrožuje turbínu i samotný generátor. Záleží pak na jejich konstrukci, zda otáčky turbíny naprázdno nepřekročí maximální otáčky, které turbína snese bez poškození.

1.3.5 Turbíny pro MVE

Jak již bylo zmíněno výše, pro konstrukci MVE v České Republice se nejčastěji používají turbíny Francisovy a Kaplanovy, méně často Bánkiho. Je to způsobeno charakterem naší krajiny a tím, že většina řek u nás pramení a ve velké toky se mění až na území sousedních států. Francisovy a Kaplanovy turbíny se většinou používají na tocích s větším spádem a větším množstvím vody. Kaplanova turbína má nejplošší charakteristiku účinnosti v závislosti na velikosti průtoku vody turbínou. Bánkiho turbína je vhodná spíše pro mikrozdroje. Jednak je díky své jednoduché konstrukci levnější, ale také není konstrukce rotoru vhodná na přenášení vysokých výkonů.

1.3.6 Netechnické hlediska provedení MVE

Technická hlediska nejsou v současné době tím jediným, co ovlivňuje provedení MVE. Nezanedbatelná je otázka finanční, která s technickými podmínkami často soupeří o první místo ve vlivu na výsledné provedení MVE. V současnosti však často vystupují do popředí i požadavky státních orgánu ochrany přírody či různých zájmových spolků. I když je MVE příkladem čistého zdroje elektrické energie, jsou těmito subjekty kladeny nejrůznější požadavky jak na místo, kde může být vybudována, tak na různé detaily jejího provedení.

Příkladem požadavků státních orgánů ochrany přírody je úsilí Správy CHKO o to, aby byl jako nutná součást MVE prosazen tzv. rybí přechod, což je vodní cesta paralelní k jezu, která má na rozdíl od jezu plynulou změnu spádu a proto nečiní rybám překážku v migraci proti proudu. Nutno zdůraznit, že problém, který rybí přechod řeší, není způsoben samotnou MVE. Příčinou je samotná konstrukce jezu. Zvláště drobní majitelé MVE většinou využívají jezy, které na řece již existují. Tím na ně spadá zodpovědnost napravit chyby způsobené při regulaci řeky v dobách dávno minulých.

Příkladem požadavků vznášených zájmovými spolky je podmínka minimálního průtoku přes korunu jezu, požadovaná Českým rybářským svazem.

1.4 Požadavky na řídicí systém MVE

Na řídicí systém samostatně ovládající MVE jsou kladeny následující požadavky:

- Zajištění bezpečného chodu soustrojí turbína-generátor a minimálního průtoku přes jez
- Regulace otevření turbín pro maximální využití dostupného množství vody
- Ukládání dat o provozu MVE pro fakturaci vyrobené elektrické energie a statistické sledování provozu MVE

Nejkritičtější je zajištění bezpečného chodu soustrojí turbína-generátor a udržení minimálního průtoku přes jez. Pokud by jej řídicí systém nedokázal zajistit, znamenalo by to ohrožení vybavení MVE, nebo dokonce životů osob. Jakým způsobem by k ohrožení došlo, je popsáno dále.

Druhý a třetí požadavek již neznamená ohrožení majetku ani osob. Dokáže-li však řídicí systém MVE samostatně správně regulovat, ušetří provozovateli práci a přinese nárůst množství vyrobené elektrické energie.

Ukládání dat o MVE ovlivňuje její provoz nepřímo. Skládá se ze tří úrovní. Zaznamenávání údajů o vyrobené elektrické energii, údajů o překročení mezních hodnot sledovaných parametrů MVE a zaznamenávání informací o chybách a poruchách řídicího systému MVE. Je tedy jasné, že z dlouhodobějšího pohledu je i třetí činnost řídicího systému MVE – ukládání informací – velice přínosná a důležitá.

Následuje detailnější rozbor jednotlivých požadavků, na řídicí systém MVE.

1.4.1 Bezpečný chod soustrojí

Zahrnuje splnění následujících podmínek:

- Turbína (tím pádem i generátor) se nikdy nedostane do nebezpečně vysokých otáček
- Generátor není přetížen – proudy všech fází ani teplota nepřekročí povolenou velikost
- Všechny fáze sítě mají správné napětí
- Všechny fáze sítě mají správnou frekvenci
- Proudy fází jsou souměrné – žádná z fází není přetížena, ani přerušena
- Hladina na koruně jezu nikdy neklesne pod minimální úroveň

Pro synchronní generátory ještě navíc:

- Velikost napětí, pořadí (souslednost) fází a frekvence vyráběného napětí je v okamžiku sfázování shodná se sítí
- Vyráběné napětí se nikdy nedostane do rozvodné sítě, není-li to bezpečné

Jednotlivé body je vhodné trochu více rozvést:

Vyráběné napětí se nikdy nedostane do rozvodné sítě, není-li to bezpečné (synchronní generátor)

Tato podmínka je obzvláště důležitá, pokud je synchronní generátor připojen do veřejné rozvodné sítě. Její nedodržení znamená možné **ohrožení života** pracovníků, kteří odstavili úsek veřejné rozvodné sítě a chystají se na něm pracovat. Generátory MVE totiž většinou vyrábějí elektrickou energii se jmenovitým napětím 3 x 400 V. To znamená, že ji dodávají do rozvodné sítě přímo. Pokud si tedy pracovníci odpojí úsek sítě například u transformátoru 22 kV/400 V, působí synchronní generátor, jako cizí zdroj, který je mimo jejich kontrolu. Nepomůže ani situace, kdy je budící napětí pro synchronní generátor tvořeno usměrněním síťového napětí. Synchronní generátor totiž vyrábí napětí až 100 V i bez budícího napětí. Příčinou je tzv. zbytkový magnetismus rotoru [Elek5]. Je proto zodpovědností provozovatele MVE, zajistit kontrolu přítomnost napětí všech fází v síti a v případě jeho výpadku okamžité odpojení generátoru.

Jiná situace je v případě provozu synchronního generátoru v ostrovní síti, kde je jediným zdrojem elektrické energie. V takovém případě jsou zase kladeny požadavky na regulaci otevření turbíny a budícího napětí generátoru. Úkolem řídicího systému potom je udržet vyráběné napětí na hodnotě U_{fef} = 3 x 400 V a frekvencí na f = 50 Hz. Není zde však potřeba řešit problém odpojování generátoru od rozvodné sítě při výpadku jejího napětí.

Turbína (tím pádem i generátor) se nikdy nedostane do nebezpečných otáček

Dodržování této podmínky již sice přímo neohrožuje lidské životy, zato však rozhoduje o životnosti soustrojí turbína-generátor.

Většina turbín má tu vlastnost, že se při výpadku zátěže roztočí na vyšší otáčky, než jsou jejich jmenovité pracovní otáčky. Zátěž může vypadnout z nejrůznějších důvodů:

- Roztržení převodového řemene od turbíny ke generátoru
- Výpadek budícího napětí z veřejné rozvodné sítě (asynchronní generátor)
- Odpojení generátoru kvůli výpadku napětí veřejné rozvodné síťě (synchronní generátor)
- Odpojení generátoru z důvodu přehřátí, překročení maximálního proudu fázemi, nesouměrnosti proudů v jednotlivých fázích, nebo nesprávné frekvence síťového napětí

Vždy záleží na konstrukci turbíny, jak velké budou její otáčky bez zatížení. V prvním případě se otáčky turbíny ustálí na zvýšené hodnotě, tzv. volnoběžné otáčky, na které je turbína konstruována a neohrožují ji. Ve druhém případě mají otáčky turbíny tendenci stále stoupat, až dojde např. k roztržení rotoru generátoru, oběžného kola turbíny, poškození ložisek,

nebo jinému poškození. I když v prvním případě k poškození turbíny nedojde, je ještě potřeba prověřit, zda zvýšené otáčky snese rotor generátoru. Z uvedeného plyne, že je velmi vhodné zajistit zavření turbíny v případě výpadku její zátěže.

Generátor není přetížen

K přetížení a/nebo přehřátí generátoru může dojít více způsoby:

- Poškození izolace jednoho z vinutí
- Zkrat na výstupu generátorů
- Poddimenzovaný generátor vzhledem k výkonu turbíny

Jak je patrné, některé příčiny přetížení mají pozvolný dlouhodobý charakter, např. přetížení v důsledku poddimenzovaného generátoru. Jiné příčiny přetížení jsou okamžité, např. zkrat na výstupu. Pozvolně se projevující přetížení dokáže spolehlivě odhalit teplotní čidlo přehřátí generátoru. Okamžité přetížení naopak odhalí ampérmetry v jednotlivých fázích.

Všechny fáze mají správné napětí a frekvenci

Tato podmínka se spíše týká kontroly parametrů veřejné rozvodné sítě. Ta totiž také musí mít správné parametry, aby k ní bylo možné generátor připojit.

Proudy fází jsou souměrné

Kromě proudu většího, než je dovolený v jedné fázi nebo několika fázích, je nutné kontrolovat i výpadky fází. Ty mohou být způsobeny přerušením statorového vinutí generátoru, nebo případně i výpadkem fází ve veřejné rozvodné síti.

Hladina na koruně jezu nikdy neklesne pod minimální úroveň

Dodržování minimálního průtoku vody se vlastně netýká bezpečného provozu samotného soustrojí turbína-generátor. Jde o dodržení požadavků kladených na provoz MVE státními orgány ochrany přírody (např. Správa CHKO), nebo různými zájmovými spolky (např. Český rybářský svaz).

Velikost napětí, pořadí (souslednost) fází a frekvence vyráběného napětí je v okamžiku sfázování shodná se sítí (synchronní generátor)

Nesplnění všech výše zmíněných předpokladů, má za následek velice působivé efekty v okamžiku připojení generátoru k rozvodné síti. V lepším případě dojde k velikému mechanickému rázu a/nebo výpadku proudových ochran (pojistek, jističů) generátoru. V horším případě proudový může ráz poškodit vinutí generátoru. K mechanickému rázu dochází proto, že neshoda parametrů výstupu generátoru a rozvodné sítě znamená, že generátor (přesněji jeho otáčky) musí být skokově urychlen, nebo přibrzděn.

Všechny tyto podmínky musí být nutně splněny pro bezpečný provoz MVE. Systém, který je zajišťuje, musí být dostatečně spolehlivý, aby dokázal zajistit jejich splnění.

1.4.2 Regulace otevření turbín

Pro maximální využití dostupného množství vody obnáší:

- Regulace otevření turbín podle aktuálního průtoku v řece
- Regulace otevření turbín tak, aby pracovaly v podmínkách, kdy mají největší účinnost (efektivitu)
- Spouštění automatického čistícího systému česlí

Provoz turbíny má různá specifika, například nejvyšší účinnosti dosahují turbíny zhruba při 80 % otevření. Je-li v MVE instalováno více turbín, je vhodné je postupně otevírat tak, aby co nejvíce z nich pracovalo se zmíněným 80 % otevřením. Při malém průtoku je výhodnější turbínu otevřít více, než dovoluje přítok řekou. Při poklesu hladiny na koruně jezu k minimální úrovni, pak turbínu opět zavřít a počkat, až nad jez doteče voda a hladina opět stoupne. Provoz v takovémto pulzním režimu ve výsledku způsobí, že MVE vyrobí více elektrické energie, než kdyby turbína pracovala s minimálním otevřením, při kterém ještě generátor vyrábí. Při malém otevření má totiž turbína výrazně menší účinnost [Elek9].

Je také nutné sledovat rozdíl hladin před a za česly na vtoku do MVE. Překročí-li rozdíl hladin velikost způsobenou samotnými česly, je nutné spustit automatický systém čištění. Čištění česlí je obzvlášť důležité na horských tocích lemovaných listnatými porosty. Zejména na jaře a na podzim totiž voda unáší velké množství listí a jiných nečistot, které česla spolehlivě ucpou. Existuje ještě možnost spouštět čistící systém česlí v určitých předem daných časových intervalech. Tato varianta je sice lepší, než žádné čištění, ale není příliš vhodná. Mechanismus čistící česla se totiž poměrně hodně opotřebovává a tak je žádané spouštět jej, jen když je opravdu potřeba. Je-li však nastaven příliš velký interval čištění, MVE pracuje kvůli ucpaným česlím se sníženým výkonem. Řešením je kontrola MVE provozovatelem zhruba jednou za dva dny, což ovšem značně degraduje výhodu automatického řídicího systému MVE. Jejím hlavním přínosem je totiž autonomní provoz MVE bez neustálého dohledu provozovatele.

1.4.3 Ukládání dat o provozu MVE

Jak již bylo zmíněno, ukládání dat o provozu MVE, ovlivňuje její chod až druhotně. Přesto by měl některé informace ukládat i základní řídicí systém MVE. Jde v prvé řadě o zaznamenávání všech chybových stavů řídicího systému, nebo jeho poruch, které je ještě systém schopen zaznamenat. Právě pomocí těchto údajů je totiž možné odhalovat chyby řídicího systému a zdokonalovat jej v odolnosti proti událostem, které konstruktéra nenapadly.

Další skupinou dat, která je vhodné ukládat, jsou hodnoty provozních veličin MVE a jejího soustrojí. Mezi ně patří:

- Okamžitý výkon jednotlivých generátorů
- Velikost otevření turbín
- Hladina vody před česly
- Hladina vody za česly
- Záznamy o spouštění čistícího systému česlí
- Otáčky turbín
- Otáčky generátorů
- Teploty turbín, teploty ložisek turbín
- Teploty generátorů, teploty ložisek generátorů

Velmi vhodné je zaznamenávat alespoň všechna překročení mezních hodnot sledovaných veličin. Lepší ale je, pokud se sledované veličiny ukládají, i když právě nevybočují ze svých normálních mezí. Jakmile potom některá hodnota vybočí z dovolených mezí, je možné sledovat, zda k překročení došlo skokově, nebo zda se sledovaná veličina pozvolně blížila k minimální nebo maximální mezní hodnotě.

Jako doplňkové je možno považovat ukládání informací o množství vyrobené energie. Tyto informace pak mohou sloužit pro účely automatické nebo poloautomatické fakturace.

Všechny ukládané informace o provozu MVE pak lze statisticky zpracovávat a získat z nich mnohé cenné závěry. Nejdůležitějším parametrem z hlediska ekonomičnosti MVE je beze sporu výkon generátorů v závislosti na čase.

Z výšky hladiny před česly a rozdílu hladin před a za česly, velikosti otevření turbín a četnosti spouštění automatického systému čištění česlí v závislosti na čase, lze vyvodit informace o množství vody v řece a množství nečistot, které voda unášela. To vše v průběhu celého roku.

2. Systémy odolné proti poruchám

V závěru předchozí kapitoly, byly rozebrány požadavky na řídicí systém MVE. Bylo jasně uvedeno, že řídicí systém musí být velice spolehlivý. Definice spolehlivosti, používaná v oblasti systémů odolných proti poruchám, bude uvedena později. I bez ní je však intuitivně jasné, že spolehlivý systém je ten, který správně **plní svou funkci**. Jelikož řídicí systém MVE není jediný systém, na který jsou kladeny požadavky na spolehlivost, je vhodné seznámit se s postupy, používanými u jiných systému na které jsou kladeny podobné požadavky. Zmíněné vysoce spolehlivé systémy se souhrnně nazývají systémy odolné proti poruchám.

2.1 Motivace: Proč se zabývat systémy odolnými proti poruchám?

Lidé jsou v současné společnosti obklopeni nespočetným množstvím technických zařízení a strojů, které jim zpříjemňují, ulehčují, nebo dokonce umožňují život. Výpadek řízení některých z nich jim v nejhorším případě způsobí nepohodlí, zdržení, či drobné finanční ztráty. Jelikož je však v současnosti technologie neodmyslitelnou součástí lidského života, existují i technická zařízení a stroje, jejichž selhání ohrožuje životy obrovského množství lidí. I laickou veřejnost v této souvislosti určitě napadne jaderná energetika nebo vojenské zbraňové systémy. Příkladů je však daleko více:

Vojenské stroje, zařízení a systémy:

- řídící jednotky letadel, vrtulníků, lodí, tanků
- řídící jednotky naváděných střel a raket
- ovládání a řízení jaderných zbraní a systémů hromadného ničení

Kosmický výzkum:

- raketoplány
- rakety
- vesmírné sondy
- Hubblův teleskop

Jiné poměrně známé aplikace systémů odolných proti chybám tvoří:

Řízení elektráren:

- jaderných
- tepelných (uhelných, plynových)
- vodních

Systémy podporující životní funkce pacientů:

- přístroje JIP (umělá ledvina, podpora dýchání, sledování srdečního tepu)
- ozařovací přístroje
- zobrazovací přístroje (rentgen RTG, počítačový tomograf CT, magnetická rezonance)

Velké koordinační systémy:

- řízení letového provozu
- řízení železniční dopravy
- řízení námořní dopravy

Aplikace, u nichž použití systémů odolných proti poruchám tak samozřejmé není, jsou například:

Řízení procesů v těžkém průmyslu:

- železárny (vysoké pece, válcovací stolice, …)
- ropný průmysl
- chemický průmysl
- zdroje pitné vody
- elektrická veřejná rozvodná síť
- síť plynového hospodářství
- čističky odpadních vod

Řízení dopravních prostředků a strojů:

- lodě
- letadla
- vlaky, metro
- automobily (řídicí jednotky ABS)
- výrobní linky a roboti

Velmi zajímavá je například oblast letadel, která jsou bez výkonného řídicího systému neovladatelná. Podobné to je s nosnými raketami vynášejícími raketoplán na oběžnou dráhu. Jejich tah je také regulován velmi výkonným řídicím systémem, aby byl dodržen přímý směr.

Komunikační a datové systémy:

- ústředny
- družice
- směrovače, routery páteřních spojů internetu
- transakční systémy pro burzy
- bankovní a jiné finanční databáze
- vládní databáze

Velké vědecké projekty:

- částicový urychlovač v CERNu
- Hubblův teleskop
- zkušební jaderné reaktory

Zmíněné systémy, které vyžadují dohled a řízení odolné proti poruchám, lze ještě dělit podle různých úhlů pohledu.

Podle způsobu, jakým je jejich selhání nebezpečné:

- systémy, jejichž selhání přímo ohrožuje velké materiální hodnoty, nebo životy zvířat, či dokonce osob
- systémy, u nichž může ohrožení velkých materiálních hodnot, nebo životů zvířat, či dokonce osob vzniknout jako druhotný následek

Do druhé skupiny patří převážně telekomunikační zařízení a různé jiné systémy, které zajišťující komunikaci, nebo přísun rozhodujících informací.

Na systém mohou být kladeny nároky, aby měl:

- nejdelší možnou životnost a provozuschopnost (například řídicí systém vesmírné sondy bez návratu)
- nejnižší pravděpodobnost výpadku plného výkonu po určitou omezenou dobu (například burzovní transakční systém, při otevření burzy, nebo řídicí systém letadla během letu)

Rozdíl mezi zařízeními je i v tom, jestli se u nich předpokládá možnost řídicí systém opravovat:

- opravované systémy
- neopravované systémy

Řídicí systém vesmírné sondy bez návratu určitě opravován nebude. Podobně tomu bude například se zesilovačem signálu, jenž je součástí podmořského kabelu. Ten je sice teoreticky možné opravovat, ale je to velmi náročné a nákladné. Jiná situace je u řídicího systému cestovního letadla. Ten nejen že se opravuje (nebo se vyměňují jeho části), ale navíc je pravidelně po určité době kontrolován jeho stav.

Všechny tyto kritické systémy jsou bez výjimky ovládány počítači. O jejich podílu na možnosti selhání vtipně hovoří následující dva citáty.

Murphyho zákon o spolehlivosti:

„Může-li se něco pokazit více způsoby, pokazí se to tak, aby to napáchalo co největší škody.“

„Chybovat je lidské, jen počítač však dokáže něco opravdu zvrtat.“ Volný překlad, viz [Fault1].

Jelikož si zmíněné skutečnosti konstruktéři uvědomují, zabývají se systémy odolnými proti poruchám.

2.2 Úvod do problematiky systémů odolných proti poruchám

Problematika systémů odolných proti poruchám je velice široká a zabývá se obrovským množstvím dílčích úkolů. Pro ukázku je zde uvedeno, co všechno do problematiky systémů odolných proti poruchám mimo jiné spadá [Fault2]:

- *ukazatele spolehlivosti, jakosti*
- *metody řízení spolehlivosti, jakosti*
- spolehlivostní modely systémů
- *zálohování*
- samo-opravné kódy
- *architektura systémů odolných proti poruchám*
- *programové vybavení systémů odolných proti poruchám*
- diagnostika systémů

Tato práce se částečně věnuje oblastem, které jsou v seznamu zvýrazněny kurzívou. Většina poznatků je čerpána z pramene [Fault2], na něj jsou odkazováni i případní zájemci o bližší informace.

2.3 Definice spolehlivosti

Spolehlivost samotná není měřitelná veličina. V normě ČSN 010102 je spolehlivost definována jako *„obecná vlastnost objektu spočívající ve schopnosti plnit požadované funkce při zachování hodnot stanovených provozních ukazatelů v daných mezích a v čase podle stanovených technických podmínek“*.

Definice je doplněna několika vysvětlujícími poznámkami:

- Spolehlivost je komplexní vlastnost, která může zahrnovat např. bezporuchovost, životnost, udržovatelnost a skladovatelnost, buď jednotlivě, nebo v kombinaci.
- Technickými podmínkami se rozumí souhrn specifikací technických vlastností, předepsaných pro požadovanou funkci objektu, dále způsoby jeho provozu, skladování, přepravy, údržby a opravy.
- Provozní ukazatele jsou ukazatele produktivity, rychlosti, spotřeby elektrické energie, paliva, apod.

Definici spolehlivosti podle normy ČSN 010102, doplňuje definice toho, co je považováno za objekt. Objekt může být libovolně malý, nebo libovolně velký celek, který je možné zkoumat současně. Např. součástka, funkční blok, jednotka, systém apod.

Jelikož je spolehlivost komplexní vlastnost, nelze ji vyjádřit jednou číselnou hodnotou, která by umožňovala seřadit všechny objekty podle jejich spolehlivosti. Namísto toho zavádí norma tzv. ukazatele spolehlivosti. Jde o veličiny, které lze jednotlivě vyhodnocovat. Ukazatele spolehlivosti jsou kvantitativním vyjádřením dílčích vlastností objektu. Dohromady ukazatele spolehlivosti popisují spolehlivost daného objektu. Definice spolehlivosti uvedená v anglicky psané literatuře je obdobná, liší se však ukazatele spolehlivosti, které jsou k jejímu popisování používány [Fault8].

Pro další studium spolehlivosti je vhodné definovat pojmy porucha a chyba. Citovaná norma definuje *poruchu* (angl. fault), jako jev spočívající v ukončení schopnosti objektu plnit požadovanou funkci podle technických podmínek. *Chyba* (angl. error) je rozdíl mezi správnou a skutečnou hodnotou nějaké veličiny, zjištěný měřením nebo pozorováním. Porucha je tedy často původcem chyby. Chyba se však může, ale také nemusí projevit např., pokud se součástka, která má poruchu, právě nevyužívá.

Objekt se může nacházet ve dvou stavech:

- poruchový stav objektu (tj. tehdy, když porucha nastala)
- bezporuchový stav objektu (tj. tehdy, když porucha nenastala)

V nejjednodušším případě zůstává systém po výskytu poruchy v poruchovém stavu až do chvíle, kdy je porucha opravena, nebo až je systém vyřazen z provozu. Taková porucha se nazývá stálá porucha. Ve skutečnosti se ale mnohem častěji setkáváme se stavem, kdy se porucha objevuje a

opět neočekávaně mizí v okamžicích, které nikdo nedokáže předpovídat. Tento typ poruchy se nazývá občasná, nebo nestálá porucha.

Výsledná spolehlivost objektu velmi závisí na tom, je-li objekt obnovovaný (hovor. opravovaný), nebo neobnovovaný (hovor. neopravovaný). Obnova je potom vlastní přechod z poruchového do bezporuchového stavu, kdežto oprava je činnost, která k obnově vedla. Objekt může být neobnovovaný, protože jej nelze opravovat (např. integrovaný obvod), je nepřístupný (kosmické sondy, přístroje na odlehlých místech Země), nebo není opravován z jiných důvodů (např. oprava je neekonomická). Tato hlediska je velmi důležité při specifikaci vlastností systémů odolných proti poruchám zohlednit.

Se spolehlivostí úzce souvisí bezpečnost provozu systému. Definuje se jako pravděpodobnost, že se na výstupu systému neobjeví nedetekovaná chyba. Tuto skutečnost nelze vyjádřit žádným ukazatelem spolehlivosti. Kromě pravděpodobnosti výskytu chyby tu hraje roli i pravděpodobnost její detekce. Velké bezpečnosti systémů se dosahuje pomocí průběžných kontrol správnosti funkce systému. Pokud výstupem těchto kontrol zastavíme činnost systému, můžeme zabránit škodlivým důsledkům, které by v řízené soustavě způsobil nesprávný řídicí signál.

Bezpečnost a spolehlivost jsou u systémů, na nichž závisí velké materiální hodnoty, životy zvířat, nebo dokonce lidí, kriticky důležité [Fault3].

2.3.1 Ukazatele spolehlivosti neobnovovaných objektů

Informace uvedené v této kapitole jsou čerpány z pramenů [Fault6, Fault7, Fault8 a Fault9]. Ukazatele spolehlivosti neobnovovaných objektů jsou veličiny náhodného charakteru, proto se pro jejich určování a práci s nimi používá pravděpodobnostní počet.

Náhodnou veličinu charakterizuje její distribuční funkce, což je pravděpodobnost, že je hodnota dané veličiny menší než určitá zadaná hodnota.

Mějme náhodnou veličinu x pro kterou platí $x > 0$, potom $F(s)$ je její distribuční funkce daná vztahem: $F(s) = P(x < s)$, kde $P(A)$ je pravděpodobnost jevu A. V tomto případě jev $\{A: x < s\}$ znamená, že náhodná veličina x je menší, než daná hodnota s. Hodnota s je nezáporné reálné číslo. Distribuční funkce $F(s)$ je neklesající kladná $(0 \leq F(s) \leq 1)$ funkce pro všechna s. V anglicky psané literatuře, se distribuční funkce nazývá *Cumulative Distribution Function* a značí se *cdf*.

Základní náhodnou veličinou v teorii spolehlivosti je velikost časového intervalu od uvedení objektu do provozu do jeho poruchy. Pokud označíme čas měřený od uvedení objektu do provozu jako t, je významným ukazatelem spolehlivosti jeho distribuční funkce $Q(t)$, který se v teorii spolehlivosti nazývá *pravděpodobnost poruchy objektu*.

Pravděpodobnost poruchy objektu $Q(t)$

$Q(t)$ je pravděpodobnost poruchy objektu do času t. V anglosaské literatuře se tento ukazatel spolehlivosti zjednodušeně nazývá unreliability (nespolehlivost) a značí se $F(t)$.

Dalším důležitým ukazatelem spolehlivosti je doplňková funkce k pravděpodobnosti poruchy objektu do času t. Jde vlastně o doplněk $Q(t)$ do jedničky, značí se $R(t)$.

Pravděpodobnost bezporuchového stavu objektu $R(t)$

$R(t)$ je pravděpodobnost bezporuchového stavu objektu do času t. V anglosaské literatuře bývá tento ukazatel spolehlivosti nazýván reliability (spolehlivost) a značí se stejně jako v české literatuře $R(t)$. Tento fakt je nutné si při čtení anglické literatury uvědomit a neplést si anglický název ukazatele spolehlivosti s českým pojmem spolehlivost, který byl definován v kapitole Spolehlivost. Občas se i v české literatuře vyskytne číselný údaj nazvaný spolehlivost. V tom případě je jím míněna právě pravděpodobnost bezporuchového stavu objektu $R(t)$. Stává se to především v českých překladech anglicky psané literatury.

Pravděpodobnost bezporuchového stavu objektu $R(t)$ lze spočítat podle vztahu:

$$R(t) = 1 - Q(t) \qquad (2.1)$$

Je-li náhodná veličina spojitá, lze z ní odvodit další důležitý ukazatel spolehlivosti. Je jím

Hustota poruch $f(t)$

Ze statistického hlediska je hustota poruch hustotou pravděpodobnosti $f(t)$ náhodné veličiny t. Anglicky se hustota pravděpodobnosti náhodné veličiny nazývá *Probability Density Function* a značí se *pdf*. Hustota poruch je definována derivací distribuční funkce podle času:

$$f(t) = \frac{dQ(t)}{dt} \qquad (2.2)$$

pokud tato derivace existuje.

V anglicky psané literatuře se hustota poruch značí failure density function, značí se stejně jako v české literatuře $f(t)$.

Součin $f(t)dt$ udává, s jakou pravděpodobností nastane ve sledovaném objektu porucha ve velmi krátkém intervalu dt následujícím za okamžikem t.

Dalším ukazatelem charakterizujícím spolehlivost objektu je:

Intenzita poruch $\lambda(t)$

Ve statistice jde o intenzitu pravděpodobnosti náhodné veličiny (zkráceně *intenzita pravděpodobnosti*). Je definována vztahem:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1-Q(t)} \qquad (2.3)$$

Intenzita poruch udává podmíněnou hustotu poruch v čase t , za předpokladu, že k poruše dosud nedošlo. V anglicky psané literatuře není název pro intenzitu poruch jednoznačný, říká se jí *hazard function*, *hazard rate*, nebo *failure rate function*. Označuje se $z(t)$. Součin $\lambda(t)dt$ udává pravděpodobnost, že se objekt, který neměl poruchu v čase t, porouchá v malém časovém intervalu dt následujícím za okamžikem t. Dosazením vztahu (2.1) do (2.2) a odtud potom do (2.3), lze prokázat, že dosud zavedené ukazatele spolehlivosti spolu těsně souvisí.

$$f(t) = -\frac{dR(t)}{dt}$$

$$\lambda(t) = -\frac{dR(t)}{dt}\frac{1}{R(t)} \qquad (2.4)$$

Diferenciální rovnici (2.4) lze upravit na tvar:

$$-\lambda(t)dt = \frac{dR(t)}{R(t)}$$

a řešit pomocí integrace od 0 do t:

$$R(t) = e^{-\int_0^t \lambda(\tau)d\tau} \qquad (2.5)$$

Empiricky bylo zjištěno, že funkce $\lambda(t)$ má průběh tzv. vanové křivky. Sestupná část vanové křivky trvá asi 6 až 10 týdnů. Doba, kdy je intenzita poruch $\lambda(t)$ téměř konstantní trvá přibližně 10 let, proto (2.5) integrujeme, jako by byla $\lambda(t)$ konstanta.

Výsledkem je vztah:

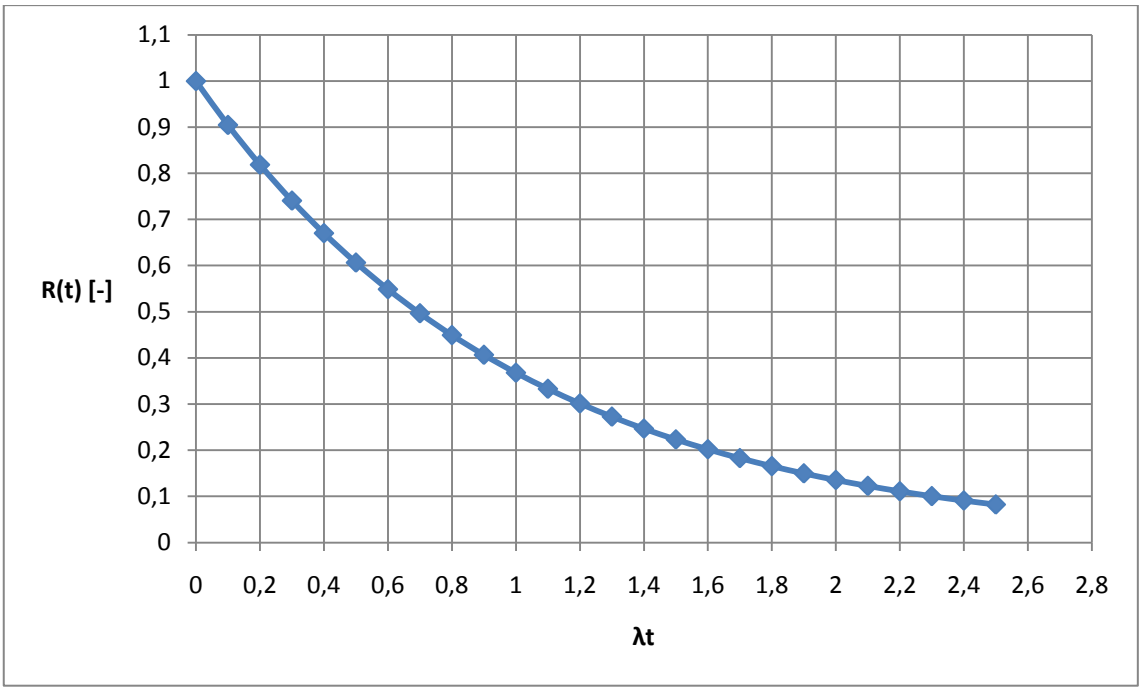
$$R(t) = e^{-\lambda(t)} \qquad (2.6)$$

Z něj lze odvodit vztahy:

$$Q(t) = 1 - e^{-\lambda(t)} \qquad (2.7)$$

$$f(t) = \lambda e^{-\lambda(t)} \qquad (2.8)$$

Vztahy (2.6) až (2.8) vyjadřují tzv. *exponenciální zákon poruch*, nebo z hlediska teorie statistiky *exponenciální rozdělení*.



Obr. 3 Exponenciální zákon poruch

Jeho grafickým vyjádřením je klesající exponenciála, viz obr. 3. Pro čas $t = 0$ má pravděpodobnost bezporuchového stavu objektu $R(0) = 1$ odpovídá to předpokladu, že objekt je na počátku měření (po uvedení do provozu) v bezporuchovém stavu. Když čas roste nade všechny meze $t \to \infty$, klesá hodnota pravděpodobnosti bezporuchového stavu objektu k nule $R(\infty) = 0$. Exponenciální závislost pravděpodobnosti bezporuchového stavu objektu na čase z obr. 3, lze chápat i jinak. V čase $t = 0$, uvedeme do provozu n zkoumaných objektů s konstantní intenzitou poruch λ. Počet objektů v bezporuchovém stavu se bude exponenciálně zmenšovat podle křivky $n_b(t) = ne^{-\lambda(t)}$.

U objektů a systémů, které budou rozebrány, se dále předpokládá konstantní velikost intenzity poruch λ a exponenciální průběh pravděpodobnosti bezporuchového stavu objektu $R(t) = e^{-\lambda(t)}$.

Střední doba bezporuchového provozu T_s

U neobnovovaných objektů též známá jako střední doba do první poruchy. V anglicky psané literatuře též jako *MTTF* (*Mean Time to Failure*). Jde o průměrnou dobu provozu objektu, během níž nenastala žádná porucha. Lze ji spočítat podle vztahu odvozeného z výrazu výpočet střední hodnoty spojité náhodné veličiny:

$$T_s = \int_0^\infty R(t)dt \qquad (2.9)$$

Za předpokladu, že je intenzita poruch λ konstantní, je znám vztah pro $R(t)$ a je možné integrál 2.9 vypočítat:

$$T_s = \int_0^\infty e^{-\lambda t}\,dt = \frac{1}{\lambda} \qquad (2.10)$$

Tento jednoduchý vztah je s oblibou používán, je však důležité mít na paměti, že oblast platnosti tohoto vztahu je omezená. Vztah poskytuje

smysluplné výsledky jen pro dobu života objektu, ve které je jeho intenzitu poruch konstantní. Pokud se například do vztahu dosadí intenzita poruch integrovaného obvodu $\lambda = 10^{-6}h^{-1}$, vychází střední doba bezporuchového provozu $T_s = 10^6 h \doteq 114\, let$. Tato hodnota je ovšem nesmyslná, protože intenzita poruch λ přestává být konstantní už asi po 10 letech.

2.3.2 Ukazatele spolehlivosti obnovovaných objektů

Informace uvedené v kapitole o spolehlivosti obnovovaných objektů, jsou opět čerpány z pramenů [Fault6, Fault7, Fault8 a Fault9]. Životní cyklus obnovovaných objektů se skládá ze sekvence časových úseků τ_{pi} – i-tá doba bezporuchového provozu a τ_{oi} – i-tá doba trvání opravy. Na začátku spustíme zařízení, které pracuje po dobu τ_{p1}, až do první poruchy. Oprava trvá dob τ_{o1}. Takto se doba bezporuchového provozu τ_{pi} a doba trvání opravy τ_{oi} neustále střídají až do ukončení provozu zařízení

Střední doba mezi poruchami T_s

Střední doba mezi poruchami se značí T_s, a je hlavním ukazatelem spolehlivosti obnovovaných objektů. Spočítáme ji jako podíl celkové doby bezporuchového provozu objektu t_p a počtu výpadků n. Celková kumulativní doba bezporuchového provozu objektu je součet všech dílčích dob bezporuchového provozu objektu τ_{pi}.

$$T_s = \frac{t_p}{n} = \frac{1}{n}\sum_{i=1}^{n} \tau_{pi} \qquad (2.11)$$

V anglicky psané literatuře se zavádí podobný ukazatel *MTBF* (*Mean Time between Failures*). Na rozdíl od střední doby mezi poruchami, užívané v české literatuře, započítává jak dobu bezporuchového provozu, tak i dobu opravy. Číselně má tedy pro stejný objekt MTBF větší hodnotu, než T_s. Českým ekvivalentem MTBF je *střední doba cyklu* T_c.

Součinitele (koeficienty) pohotovosti $K_p(t)$ a prostoje $K_n(t)$.

Součinitel pohotovosti $K_p(t)$

$K_p(t)$ se nazývá okamžitý součinitel pohotovosti a určuje pravděpodobnost toho, že v čase t bude systém provozuschopný. Většinou existuje limita $K_p = \lim_{t\to\infty} K_p(t)$, která se označuje jako stacionární součinitel pohotovosti. Hodnota stacionárního součinitele pohotovosti udává pravděpodobnost toho, že systém v ustáleném provozním stavu bude provozuschopný v libovolném zvoleném okamžiku. Prakticky lze stacionární součinitel pohotovosti považovat za poměrnou část provozuschopné doby z celkové sledované doby.

$$K_p = \frac{t_p}{t_p + t_o} \qquad (2.12)$$

Kde t_p je celková doba provozu objektu a t_o je celková doba opravy objektu za sledované období.

Střední doba opravy T_o

Je to průměrná délka trvaní opravy objektu ve sledovaném období. Definujeme ji jako podíl celkové doby opravy a počtu poruch:

$$T_o = \frac{t_o}{n} \tag{2.13}$$

V anglicky psané literatuře, se střední doba opravy nazývá *mean time to repair*, zkratka *MTTR*. Jestliže dobu trvání opravy považujeme za náhodnou veličinu s exponenciálním rozdělením pravděpodobnosti, lze pro ni vyjádřit intenzitu pravděpodobnosti náhodné veličiny. V teorii spolehlivosti se nazývá *intenzita oprav* a značí se μ. Předpokládá se, že intenzita oprav μ je konstanta. Střední dobu opravy pak lze vyjádřit vztahem:

$$T_o = \frac{1}{\mu} \tag{2.14}$$

Po dosazení vztahů 2.11, 2.13 a 2.14 do vztahu 2.12 vyjde:

$$K_p = \frac{T_s}{T_s + T_o} = \frac{\mu}{\mu + \lambda} \tag{2.15}$$

Součinitel prostoje $K_n(t)$

Okamžitý součinitel prostoje $K_n(t)$ je doplňkem okamžitého součinitele pohotovosti do jedné:

$$K_n(t) = 1 - K_p(t) \tag{2.16}$$

Stacionární součinitel prostoje K_n je určen limitou $K_n = \lim_{t\to\infty} K_n(t)$. Tento ukazatel spolehlivosti, určuje pravděpodobnost, že v libovolně zvoleném okamžiku nebude systém provozuschopný.

Definice pravděpodobnosti bezporuchového stavu objektu $R(t)$ a součinitele pohotovosti $K_n(t)$ se mohou zdát podobné, je mezi nimi však značný rozdíl. Pravděpodobnost bezporuchového stavu objektu $R(t)$ udává pravděpodobnost, že nedošlo k poruše objektu v celém intervalu $< 0, t >$. Naproti tomu součinitel pohotovosti hodnotí, jestli je objekt v bezporuchovém, nebo v poruchovém stavu, buď v jednom náhodně zvoleném okamžiku (okamžitý součinitel pohotovosti $K_p(t)$), nebo statisticky srovnává doby, kdy je objekt v bezporuchovém stavu a kdy je v poruchovém stavu (stacionární součinitel spolehlivosti K_p). Požadavky na zkoumaný objekt, vyjádřené pravděpodobností bezporuchového stavu objektu $R(t)$, jsou mnohem přísnější, než požadavky vyjádřené součinitelem pohotovosti (ať už okamžitým $K_p(t)$, nebo stacionárním K_p).

Součinitel technického využití K_{tv}

Součinitel technického využití je dalším ukazatelem spolehlivosti obnovovaných objektů. Kromě celkové doby provozu t_p a celkové doby opravy t_o zahrnuje ještě celkovou dobu plánované údržby t_u. Součinitel technického využití objektu je definován vztahem:

$$K_{tv} = \frac{t_p}{t_p + t_o + t_u} \tag{2.17}$$

2.3.3 Řízení spolehlivosti

Podkladem k této kapitole jsou informace z pramene [Fault4]. Uživatelé přirozeně požadují, aby mělo zařízení co největší spolehlivost. Aby se však zvýšila spolehlivost, je obvykle nutné současně zlepšit všechny ukazatele spolehlivosti. To je však většinou nerealizovatelné, nebo realizovatelné jen v omezené míře. Výhodné je snížení hodnoty intenzity poruch λ, tím je automaticky dosaženo zlepšení hodnoty všech důležitých ukazatelů spolehlivosti (zvýší se pravděpodobnost bezporuchového stavu objektu, prodlouží se střední doba bezporuchového provozu, zvýší se hodnota součinitele pohotovosti atd.). Metody snižování intenzity poruch jsou však velmi složité a nákladné.

Metody a opatření k snižování intenzity poruch se nazývají *předcházení poruchám* (angl. *Fault Avoidance*). Použití těchto metod však má své limity, od jistého okamžiku už totiž rostou náklady na další snižování poruch neúměrně rychle. Dalším omezením jsou fyzikální překážky, které se vymykají možnostem konstruktéra, resp. jeho znalostem.

Další zvyšovaní spolehlivosti je již nutné zajistit jiným způsobem. Jedním z nich je výskyt poruch připustit a počítat s ním při návrhu a realizaci systému. Místo vyloučení poruch součástek se tedy pozornost zaměřuje na to, aby se tyto poruchy neprojevily na celkovém chování systému, případně aby se projevily jen minimálně. Zmíněný způsob vyrovnávání se s poruchami se označuje jako *odolnost proti poruchám*, nebo *tolerance poruch* (angl. *Fault Tolerance*). Systém, který na poruchy tímto způsobem reaguje, se pak nazývá *systém odolný proti poruchám* (angl. *Fault-tolerant Systém*). Při hodnocení spolehlivosti systému odolného proti poruchám je nutné rozlišovat poruchu součástky systému a poruchou celého systému, označovanou též jako *selhání systému* (angl. *Failure*). Porucha systému je taková porucha jeho součástek, která způsobí nepřijatelnou změnu jeho chování. Systém pak není schopen plnit požadovanou funkci, jak bylo popsáno v definici v kapitole Spolehlivost. Dále je potřeba upravit i způsoby výpočtů jednotlivých ukazatelů spolehlivosti (např. střední doba mezi poruchami bude měřena pouze mezi poruchami systému jako celku apod.).

Různé metody tolerance poruch se vyznačují společnou vlastností, nerovnoměrným vlivem na jednotlivé ukazatele spolehlivosti objektu. Metoda, která zlepší jeden požadovaný ukazatel spolehlivosti, jiné ukazatele zlepší jen nepatrně, ponechá je beze změny, nebo je dokonce zhorší. Vybraná metoda tolerance poruch je pak výsledkem kompromisu mezi požadavky kladenými na hodnoty jednotlivých ukazatelů spolehlivosti. Dále je vybraná metoda tolerance samozřejmě ovlivněna maximální cenou, rozměry, spotřebou energie apod. Jelikož zavádění metod tolerance poruch nezlepšuje všechny ukazatele spolehlivosti zároveň, nejedná se o zvýšení spolehlivosti. Výstižnější označení je *řízení spolehlivosti*.

2.3.4 Předcházení poruchám

Informace uvedené v této kapitole jsou čerpány z pramene [Fault5]. Metody předcházení poruchám již byly teoreticky podrobně rozpracovány, ale jejich uplatňování v praxi stále není uspokojivé. Překážky jsou zejména organizační, případně ekonomické. Dalším problémem jsou zmíněné fyzikální překážky. Pro projekty, kde jsou na spolehlivost kladeny extrémní požadavky, jsou výrobci schopni zajistit součástky s hodnotami ukazatelů spolehlivosti o několik řádů lepšími, než je běžný standard. Zvýšení spolehlivosti je však dosaženo na úkor značného zvýšení ceny. S takovou extrémní spolehlivostí však nemůže konstruktér běžných projektů počítat. Existuje však řada opatření, pomocí kterých lze u sériově vyráběných součástek zajistit co nejvyšší spolehlivost při udržení rozumných nákladů. Tyto opatření rozhodně nepatří mezi přežitky, metody tolerovaní poruch totiž dokážou maskovat jen omezený počet poruch, takže je stále důležité používat co nejspolehlivější součástky. Obecně je třeba využít všech dostupných metod předcházení poruchám (metody zvyšování spolehlivosti) a pokud ukazatele spolehlivosti objektu stále nevyhovují, aplikují se metody zajišťující toleranci poruch (metody řízení spolehlivosti). Je tedy důležité, aby se každý konstruktér nejdříve seznámil s nejdůležitějšími metodami předcházení poruchám, ještě než začne používat metody řízení spolehlivosti.

Poruchám lze předcházet při návrhu systému, jeho výrobě i provozu. Při návrhu je důležité zvolit spolehlivou součástkovou základnu a spolehlivou technologii. Při výběru součástek i výrobní technologie je třeba zohlednit podmínky, v nichž má výsledný systém pracovat. U součástek je důležité volit optimální pracovní body z hlediska výkonu (např. nevyužívat plně dovolenou zatížitelnost výstupů), tepelného režimu (např. zajistit dostatečné chlazení), dále z hlediska napájení, odrušení, pracovní frekvence, apod.

Při sériové výrobě hraje důležitou roli vstupní kontrola součástek, polotovarů a použitých materiálů. Např. z výzkumu firmy DEC plyne, že 2,5% procenta všech součástek od subdodavatelů je vyřazeno. Mezi převzatými součástkami je pak vadných už jen 0,04%. Cenu za tyto kontroly je možno chápat, jako cenu za zvyšování spolehlivosti. Výrobci se snaží zajišťovat spolehlivost především velkou technologickou kázní, sledovanou průběžnými mezioperačními kontrolami. Výsledné výrobky jsou navíc podrobovány tzv. spolehlivostním testům, při nichž jsou zkoušeny za zvýšené, případně snížené teploty, při zvýšeném napětí, při vibracích apod.

Pro předcházení poruchám jsou velmi účinné různé teplotní cykly, protože při nich se projeví skryté poruchy, které by jinak mohly ovlivnit funkci výrobku až během jeho použití. Pomocí teplotních cyklů se dosahuje zkrácení klesající části křivky intenzity poruch. Tato část je nazývána období časných poruch (angl. Infant mortality phase). Cílem je, aby v době, kdy je výrobek používán zákazníkem, měly už součástky konstantní intenzitu poruch. Při navrhování teplotních cyklů je nutné detailně znát fyzikální děje, probíhající v součástkách. Špatně navržený, nebo nedbale

provedený teplotní cyklus, může spolehlivost součástek naopak zhoršit, protože může v součástce spustit nový degradační proces.

Jednou z významných metod předcházení poruchám je zvyšování stupně integrace polovodičových součástek. Vývody pouzder integrovaných obvodů totiž patří k nejporuchovějším částem integrovaných obvodů. Snižováním počtu pouzder ubývá nespolehlivých míst.

Při vlastním provozu zařízení je pro předcházení poruchám nejdůležitější dodržování technických provozních podmínek. Mezi ně patří požadavky na klimatizaci (teplota vlhkost, prašnost vzduchu), intenzitu rušení (ze sítě i přímým vyzařováním z jiných zdrojů), stabilitu napájení, apod. Pokud to výrobce zařízení předepsal, je důležité provádět preventivní kontroly a výměny částí zařízení.

Zde je nutné upozornit, že předepisování kontrol a výměn by mělo být skutečně uvážené. Obzvláště v naší zemi a jiných post komunistických zemích je obvyklé, že pokud jsou kontroly a výměny předepsány přehnaně často, obsluhující pracovníci mají tendenci je nerespektovat a intervaly protahovat. Na výpadcích systémů se často podílí i selhání lidského faktoru – obsluhy, je proto důležité navrhovat veškeré uživatelské rozhraní intuitivní, přímočaré a přehledné.

2.3.5 Odolnost proti poruchám

Podklady pro tuto kapitoly byly čerpány z pramenů [Fault10 a Fault17]. Systém se označuje jako odolný proti poruchám, jestliže je schopen správně vykonávat svou funkci i přesto, že se v něm vyskytly poruchy technického vybavení, nebo chyby v programech. Jelikož lze termín „správně vykonávat funkci“ chápat různě, je potřeba upřesnit, kdy je funkce systému považována za správnou. Obvykle se vyžaduje splnění těchto tří podmínek:

- zpracování dat nebylo zastaveno ani změněno v důsledku poruchy
- výsledek je správný
- výsledek byl získán v předepsané době

Pokud jsou splněny jen některé z uvedených požadavků (např. správný výsledek, ale dodaný pozdě), označuje se systém jako částečně odolný proti poruchám. První podmínka, zachování funkčnosti programu, se považuje za dominantní, takže musí být splněna i u systémů částečně odolných proti poruchám.

Možná překvapí, že první počítač odolný proti poruchám na světě byl postaven v Československu na počátku 50. let. Jednalo se o reléový počítač SAPO, navržený kolektivem pracovníku Výzkumného ústavu matematických strojů v Praze pod vedením docenta Antonína Svobody. Obsahoval tři aritmeticko-logické jednotky spojené do systému TMR, o němž bude řeč později. John von Neumann popsal tento způsob zálohování až v r. 1956. Počítač SAPO ovšem obsahoval i jiné metody pro zotavení po poruše, např. opakování instrukce.

Konstruktéři, kteří pracovali na projektech systémů odolných proti poruchám, z nichž mnohé byly realizovány a vyzkoušeny, vypracovali

poměrně promyšlenou metodiku návrhu. Zmíněná metodika je však heuristickým postupem založeným na postupném přibližování se k výsledku. Jeho aplikace vyžaduje značnou míru zručnosti a zkušeností, navíc nelze nikdy dopředu určit, jestli bude dosaženo zvoleného cíle. V současné době a s dosavadními znalostmi, však není dostupná lepší metoda.

Při návrhu systému odolného proti poruchám se obvykle vychází z neodolného systému s minimem prostředků, který je schopen vykonávat požadované funkce. Z tohoto prvotního návrhu se pak úpravami a obměnami postupně vytváří systém, který se co nejvíce blíží určeným požadavkům na spolehlivost, při současném dodržení omezujících podmínek.

Systém odolný proti poruchám prochází při svém vývoji následujícími fázemi:

1. stanovení cílů
2. volba metod detekce poruch
3. návrh algoritmů zotavení po poruše
4. vyhodnocení odolnosti proti poruchám

Stanovení cílů

Správná formulace zadání pro návrh systému odolného proti poruchám je velice důležité. Vzhledem k tomu, že systém nemůže být navržen jako odolný proti všem možným typům selhání, je podstatné co nejpřesněji popsat, za jakých okolností má být systém schopný vykonávat svou funkci. V praxi jde o vytvoření co nejúplnějšího seznamu všech poruch, které mohou při provozu systému nastat. Následně je potřeba roztřídit je podle pravděpodobnosti, s jakou mohou nastat, případně podle toho, jak na ně má systém reagovat. Pokud jako reakci na některé poruchy připustíme omezení funkceschopnosti systému, je nutné dostatečně přesně popsat všechny přípustné změny, např. pokles výkonnosti, prodloužení doby reakce, omezení počtu funkcí, které systém dokáže vykonávat atd.

Je také důležité stanovit metodiku, pomocí níž se bude hodnotit odolnost výsledného systému proti poruchám.

Detekce poruch

Pro zajišťování odolnosti systému má detekce poruch klíčový význam, systém je totiž schopen správně reagovat jen na ty poruchy, o kterých je dostatečně přesně informován. Pro návrh způsobů detekce poruch, je vhodné vycházet ze seznamu poruch sestaveného při stanovování cílů. Je potřeba rozhodnout jak rychle má systém na jednotlivé poruchy reagovat, jaké k tomu má prostředky atd.

Zotavení po poruše

Jde o klíčovou část návrhu systému odolného proti poruchám, jde o vlastně o hlavní nástroj odolnosti proti poruchám. Má proto určující význam pro kvalitu výsledného systému. Zotavení po poruše zahrnuje všechny úkony, které je třeba provést od okamžiku zjištění poruchy, do obnovení funkce systému.

Rozlišují se tři druhy zotavení po poruše:

- zotavení do původní úrovně funkceschopnosti
- zotavení do degradovaného stavu
- bezpečné ukončení funkce

Jelikož to nemusí být na první pohled patrné, je vhodné zdůraznit, že obvodové maskování chyby také patří k zotavovacím mechanismům. Je specifické tím, že u něj nedochází k detekci poruch. Je to nejdokonalejší, nejrychlejší, avšak také nejnákladnější forma zotavení. Její hlavní předností, pro kterou bývá využívána je, že se porucha neprojeví chybou na výstupu takto zodolněného systému.

Vyhodnocení odolnosti proti poruchám

Jde o kontrolu, do jaké míry se podařilo splnit stanovené cíle. Vyhodnocování odolnosti ztěžuje fakt, že s formulací požadavků na odolnost i s jejich ověřováním, jsou zatím poměrně malé zkušenosti. Je proto nutné, aby se při vyhodnocování odolnosti používaly stejná kritéria, jako při stanovování cílů. Používají se analytické metody, tedy výpočty, dále simulační metody a hlavně ověřování na funkčním vzoru. Pro názornost se někdy užívají pomocné součinitele udávající poměrné změny některých důležitých ukazatelů. Příkladem je součinitel zvýšení spolehlivosti a součinitel prodloužení mise.

Součinitel zvýšení spolehlivosti $K_R(t)$ je definován vztahem:

$$K_R(t) = \frac{R_Z(t)}{R(t)} \qquad (2.18)$$

Jde tedy o podíl pravděpodobnosti bezporuchového provozu zálohovaného a nezálohovaného systému v čase t.

Součinitel prodloužení mise $K_T(R_{min})$ je definován vztahem:

$$K_T(R_{min}) = \frac{T_Z(R_{min})}{T(R_{min})} \qquad (2.19)$$

Udává, kolikrát se prodlouží doba, během které pravděpodobnost bezporuchového stavu klesne pod stanovenou mezní hodnotu R_{min}. $T(R_{min})$ je doba poklesu pravděpodobnosti bezporuchového provozu nezálohovaného systému na R_{min} a $T_Z(R_{min})$ doba poklesu téže pravděpodobnosti zálohovaného systému.

Vyhodnocení odolnosti výsledného systému je podkladem pro upřesňování a zdokonalování projektu. Výsledky totiž většinou nesplňují požadavky zadání. Opakující se proces zdokonalování systému a vyhodnocování jeho parametrů, vede v příznivém případě k přiblížení se stanoveným cílům. V opačném případě vede proces k závěru, že za daných podmínek a s prostředky, které jsou k dispozici, nelze stanovených cílů dosáhnout.

2.4 Zálohování

Teorie zálohování je čerpána z pramene [Fault11]. Odolnosti proti poruchám nelze dosáhnout jinak, než tím, že použijeme nadbytečné bloky, nazývané *záloha*. V podobné souvislosti se používá i termín redundance, ten je ale obecnější. Zálohy jsou takové nadbytečné prostředky, které jsme do systému přidali pro případ poruchy některé z jeho částí. Systém by bez poruchy pracoval správně, i kdyby záložní bloky nebyly připojeny. Redundance může také znamenat přidání bloků kvůli odolnosti proti poruchám, může však vzniknout i neúmyslně a nezvyšovat odolnost proti poruchám. K popisu teorie záloh je použito obecných pojmů, aby byl popis nezávislý na úrovni, na které bude ve skutečnosti záloha realizována. Celek, jenž je předmětem zkoumání, je nazván *systém*. Části, ze kterých je systém složen, jsou nazvány *prvky*. Pro lepší reálnou představu je možné např. za systém dosadit řídicí počítač a za prvky jednotlivé součástky, ze kterých je složen. Dělení na *systém* a *prvky* je ale univerzálnější, ve zmíněném příkladě s řídicím počítačem můžeme např. za prvky místo součástek označit bloky: paměť, procesor, vstupně výstupní obvody. Proto je dále v textu použito toto obecnější rozlišení. V případě pochybností je však vždy možno pro lepší představu dosadit za *systém* a *prvky* konkrétní příklady.

2.4.1 Klasifikace zálohy podle různých hledisek

Zálohy je možno rozlišovat a třídit podle různých kriterií. Některé z nich, jsou na sobě nezávislé, takže je možné kombinovat. Zde je uveden pohled na druhy záloh z hlediska:

- použitých prostředků
- stupně využití zálohy v čase
- úroveň využití zálohování
- vztahu záložního a zálohovaného prvku
- funkce zálohy

Použité prostředky

Zálohu lze vytvořit pomocí těchto systémových zdrojů:

- technické vybavení (software)
- programové vybavení (hardware)
- informace
- čas

Jednotlivé prostředky se většinou kombinují a nelze je oddělit. Nejpoužívanější a na představu nejjednodušší je využití nadbytečného technického vybavení. Do této kategorie patří např. záložní součástky, obvody a funkční bloky. Nadbytečné technické vybavení nejvíce zvyšuje náklady na realizaci systému, jeho rozměry, hmotnost a spotřebu energie.

Nadbytečné programové vybavení bývá spojeno s nadbytečným technickým vybavením. I když jej je možné použít i v nezálohovaných systémech. Do této kategorie patří hlavně programy na detekci a lokalizaci poruch a programy pro řízení zotavení po poruše, připojující bezporuchové bloky

namísto poruchových. V nezálohovaných systémech je možné pomocí kontrolního, nebo opakovaného výpočtu odhalit, nebo dokonce opravit chyby vznikající v systému. Z uvedeného plyne, že nadbytečné programové vybavení většinou způsobuje i využití značného množství nadbytečného času. Čas samotný se jako prostředek zálohy nepoužívá, je důsledkem použití jiného druhu nadbytečnosti, zejména nadbytečného programového vybavení.

Nadbytečné informace se využívají ve spojení s nadbytečným technickým vybavením v různých bezpečnostních kódech k průběžné detekci chyb.

Stupeň využití zálohy v čase

V tomto ohledu, se rozlišují se dva druhy zálohy:

- statická
- dynamická

Statická záloha je trvale připojena na vstupy a výstupy zálohovaného systému a je trvale zpracovává tytéž data. Nazývá se také záloha bez přepínání. Její velikou výhodou je tedy její okamžitá dostupnost. Ve skutečnosti statická záloha zaručuje maskování chyb na výstupu systému. Její hlavní nevýhodou, je velká spotřeba elektrické energie, v podstatě až dvojnásobná vůči nezálohovanému systému, protože je trvale pod zátěží. Dále pak malá doba bezporuchového provozu, právě kvůli trvalému zatížení, které ji opotřebovává stejně, jako zálohovaný systém.

Dynamická záloha je naopak odpojena od výstupů zálohovaného systému a začíná se využívat teprve, až dojde k jeho poruše. Dynamická záloha může být provozována jako nezatížená (studená), odlehčená (vlažná), nebo zatížená (horká). Studená záloha je v době správné funkčnosti zálohovaného systému odpojená od elektrické energie. Vlažná záloha je sice připojena k napájení, ale pracuje jen se sníženým výkonem. Většinou je čas od času aktualizován její stav se stavem zálohovaného systému, aby byla připravena pro převzetí funkce při výpadku zálohovaného systému. Horká záloha pracuje s plným zatížením, avšak její výstup není připojen k výstupu zálohovaného systému, dokud v něm není detekována porucha. Jak je patrné, hlavní výhodou dynamické zálohy (s výjimkou horké) oproti statické záloze, je menší spotřeba elektrické energie a delší doba bezporuchového provozu, protože záloha pracuje s menším zatížením. Nevýhodou naopak je složitá konstrukce přepínače a jeho řízení, dynamická záloha se vyplatí až v případě, kdy je zálohovaný systém výrazně složitější, než přepínač a jeho řízení. Další velkou nevýhodou dynamické zálohy je, že než řídicí obvod přepínače detekuje chybu v zálohovaném systému, může signál na výstupu na chvíli vypadnout, nebo se dokonce na výstup může dostat chybná hodnota.

Úroveň využití zálohování

Rozdělení záloh z tohoto pohledu rozlišuje, jak veliké, nebo malé, jsou zálohované bloky ve srovnání s celým systémem. Tedy jestli například zálohujeme celé funkční bloky systému, podobvody funkčních blokům nebo

dokonce jednotlivé součástky. Úroveň využití zálohování má výrazný vliv na cenu a složitost výsledného systému. Čím větší celky jsou zálohovány, tím větší je pravděpodobnost, že budou opakovány i bloky, které zálohovat nepotřebují. Úroveň využití zálohování má také vliv na složitost řízení, čím více prvků (malých bloků, ze kterých je systém složen) je zálohováno, tím složitější je řídicí podsystém, který zálohy řídí a připojuje. Úroveň využití zálohování má vliv i na účinnost zálohy, tedy na počet a typ poruch, ze kterých se systém dokáže zotavit.

Zálohovat lze tak, že se k určitému prvku přidá jeden, nebo několik záložních prvků. Například k *prvku* řídicí počítač, jenž je součástí nějakého většího *systému*, je přidán další, záložní řídicí počítač. Druhou možností, je změnit vnitřní konstrukci *prvku*. Například přidáním záložní paměti k operační paměti řídicího počítače. Zde se ukazuje univerzálnost termínů *systém* a *prvek*. Zásah do vnitřní struktury řídicího počítače přidáním paměti, lze chápat i jako zdvojení *prvku* paměť v *systému* řídicí počítač. Trik je v tom, že úroveň využití zálohování posunula o jednu níže. Tedy, že řídicí počítač, jenž byl *prvkem* většího *systému*, je nyní sám *systémem*. Jeho součásti, jako procesor a paměť, jsou nyní jeho *prvky*. Prvek paměť byl v tomto příkladu zálohován zdvojením.

Vztah záložního a zálohovaného prvku

Záložní prvek může být:

- konfigurační (masivní)
- funkční

Konfigurační záložní prvek je totožný se zálohovaným prvkem, jak svou funkcí, tak provedením a strukturou.

Funkční záložní prvek může mít jinou strukturu i provedení, podmínkou však je, aby vykonával stejnou funkci, jako zálohovaný prvek. Může však mít jiné parametry, než zálohovaný prvek, například nižší výkon.

Funkce zálohy

Účelem každé zálohy je samozřejmě zajistit odolnost systému proti poruchám, k tomuto účelu však může záloha přispívat různými způsoby:

- detekcí poruchy
- maskováním poruchy
- umožněním zotavení po poruše

Detekce poruchy je základem pro jakýkoliv systém odolný proti poruchám. Tento blok tedy nesmí chybět v žádném takovém systému, ať už je pak porucha maskována, systém přejde do degradovaného stavu, nebo je bezpečně ukončena jeho činnost.

Maskování poruchy je nejdokonalejším druhem odolnosti proti poruchám, jelikož nedovolí, aby se chybná hodnota dostala na výstup systému. Systém s maskováním poruch rovněž nepodléhá degradaci výkonu, ani množstvím funkcí, které je schopen provádět.

Zotavení po poruše nalézá své uplatnění tam, kde není zajištění maskování poruchy nutné, nebo je to silně neekonomické. Například u velmi rozsáhlých systémů.

2.4.2 Záloha typu TMR

Jde o systém se statickou zálohou, realizovaný paralelním spojením výstupů tří prvků v hlasovacím bloku, tzv. majoritním bloku. Hlasovací blok pracuje tak, že na jeho výstupu se objeví ta hodnota, která se vyskytne na třech nebo alespoň dvou vstupech zároveň. Znamená to, že systém je schopen maskovat chybný výstup jednoho z prvků. Pokud by byl chybný výstup na dvou prvcích, dostala by se chybná hodnota i na výstup hlasovacího bloku. Vstupy jednotlivých prvků systému TMR mohou být buď také paralelně spojeny, nebo je zároveň použito i více čidel dodávajících vstupní údaje. Název systému TMR je zkratkou z anglického Triple Modular Redundant. Tento systém je v praxi velmi často používán, například pro zálohování palubních počítačů vojenských i civilních letadel. Funkce hlasovacího obvodu je pro jednoduchost uvedena pro případ, kdy jsou výstupem každého ze tří bloků F_1, F_2,F_3 jednobitové signály f_1,f_2 f_3. Tyto výstupy jsou přivedeny do tří-vstupového hlasovacího bloku, který se signály provádí funkci $f = f_1 f_2 + f_2 f_3 + f_1 f_3$. Pokud mají jednotlivé bloky systému TMR n výstupů, je zapotřebí n tří-vstupových hlasovacích bloků. Výstupy hlasovacích bloku pak vytvoří n-bitový vektor výstupních signálů.

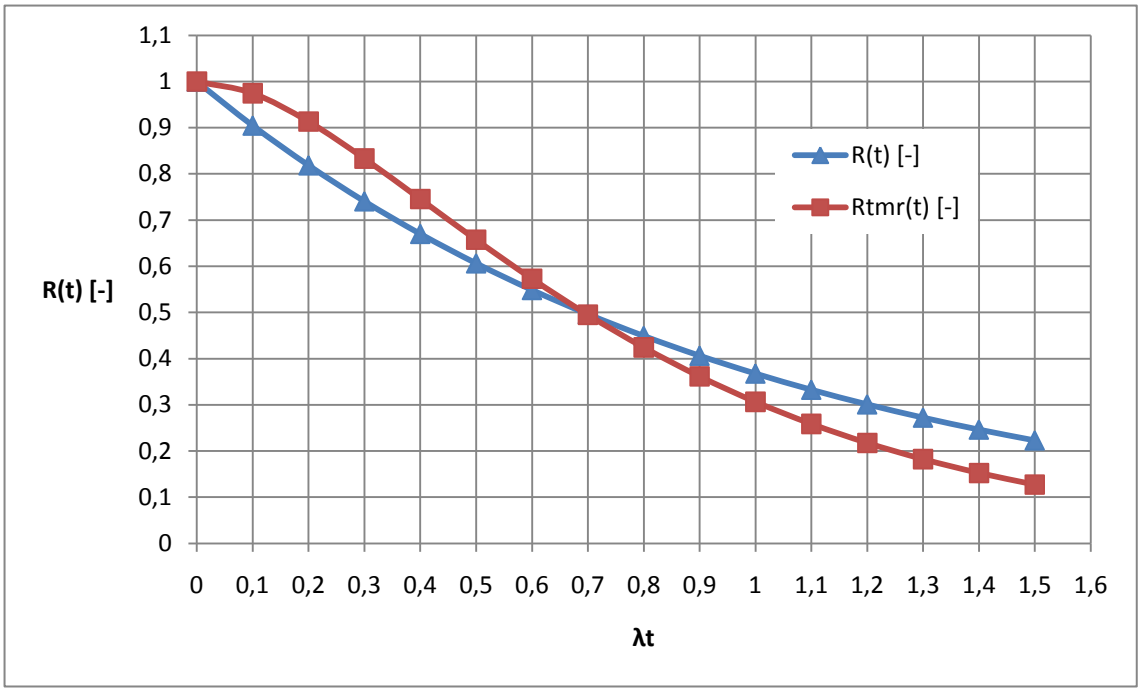
Pro výpočty ukazatelů spolehlivosti systému TMR se vychází z předpokladu, že porucha každých dvou prvků vede k chybnému výsledku na výstupu hlasovacího modulu. To je jisté zjednodušení, protože poruchy prvků se mohou za určitých okolností vzájemně kompenzovat, zde je na místě připomenout citát Murphyho zákona z motivačního úvodu v kap. 2.1Murphyho. Dochází tím k drobné nepřesnosti, která však způsobí, že ve skutečnosti, bude pravděpodobnost bezporuchového stavu systému TMR o něco lepší, než vypočtená hodnota. Pro výpočet pravděpodobnosti bezporuchového stavu systému TMR je využit vztah sčítající pravděpodobnost výskytu vzájemně se vylučujících jevů, odvozený v pramenu [Fault12]. Aplikací vztahu na případ systému TMR vznikne vztah:

$$R_{TMR}(t) = 3[R(t)]^2 - 2[R(t)]^3 \qquad (2.20)$$

Za předpokladu, že pro všechny prvky systému TMR platí exponenciální zákon průběhu pravděpodobnosti bezporuchového provozu s konstantní intenzitou poruch λ lze vztah 2.20 upravit na tvar:

$$R_{TMR}(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t} \qquad (2.21)$$

Na obr. 4 jsou znázorněny průběhy pravděpodobnosti bezporuchového provozu pro nezálohovaný systém (křivka s trojúhelníky) a systém TMR (křivka se čtverci).



Obr. 4 Pravděpodobnost bezporuchového provozu systému TMR

Ze začátku je pravděpodobnost bezporuchového provozu systému TMR větší, od hodnoty $t = 0{,}7\,T_s$ se však křivky pro nezálohovaný systém a TMR protínají a s rostoucí dobou t klesá pravděpodobnost bezporuchového stavu $R_{TMR}(t)$ systému TMR rychleji, než u nezálohovaného systému. Znamená to, že od jistého okamžiku je pravděpodobnost bezporuchového stavu systému TMR nižší, než u nezálohovaného systému. Integrací vztahu 2.21 leze odvodit hodnotu střední doby bezporuchového provozu systému TMR:

$$T_{s(TMR)} = \frac{5}{6\lambda} \qquad (2.22)$$

Znamená to, že střední doba bezporuchového provozu je zhruba 83% hodnoty střední doby provozu nezálohovaného systému. Plynou z toho dva závěry:

- Neobnovovaný systém TMR je vhodný v případě, kdy je potřeba na krátkou dobu výrazně zvýšit pravděpodobnost bezporuchového provozu.
- Pro systémy s delší dobou provozu, lze nepříjemnou vlastnost systému TMR odstranit tím, že bude provozován jako obnovovaný.

Z druhého závěru plyne, že pokud bude vadný prvek systému TMR brzy po výskytu poruchy opraven, je možné dlouhodobě systém udržovat ve stavu s vyšší pravděpodobností bezporuchového provozu, než je tomu u nezálohovaného systému.

2.4.3 Systém SIFT

Informace uvedené v této kapitole, jsou čerpány z pramenů [Fault13, Fault14, Fault15, Fault18]. Název SIFT je zkratka z anglického Software Implemented Fault Tolerance. Původně se tak nazýval vysoce spolehlivý palubní počítač pro civilní letadla vyvinutý na zakázku NASA výzkumným ústavem SRI International v Menlo Park v Kalifornii. Požadovaná intenzita poruch byla $\lambda = 10^{-9}\, h^{-1}$ po dobu $10\, h$. V tomto projektu bylo hlavním prostředkem použitým k dosažení odolnosti proti poruchám programové vybavení. Později se zkratka SIFT začala užívat jako obecný název pro zajišťování odolnosti proti poruchám programovými prostředky. Jednou ze základních úloh problematiky SIFT je realizace majoritního hlasovacího bloku programově. Tento programový majoritní hlasovací blok, lze využít například v systému TMR, který byl rozebrán v předchozí kapitole. Jednotlivé prvky systému potom nejsou připojeny k oddělenému hlasovacímu bloku, ale hlasování je prováděno programově vzájemnou komunikací jednotlivých prvků mezi sebou. Komunikace mezi prvky většinou probíhá v předem daných časových intervalech. Pokud je některý prvek rychlejší než ostatní, počká na jejich výsledky v čekací smyčce. Tomuto principu synchronizace mezivýsledků se říká volně vázané prvky.

Problém sjednocení výsledků jednotlivých prvků popsali jako první L. Lamport, R. Shostak a M. Pease, zaměstnanci firmy SRI International. Nazvali jej The Byzantine Generals Problem, zkráceně BGP.

Problém je popsán na případu generála, který obléhá město a rozhoduje se mezi útokem a ústupem, o svém rozhodnutí potřebuje informovat i všechny své poručíky. Někteří z nich (včetně generála) však mohou být zrádci. Zpráva, která pochází od zrádce, nebo přes něj putuje, může být zfalšována.

Popsáno technickými termíny, generál je *zdrojový proces*, který předává *zprávu*. Falešní generálové a poručíci jsou *poruchové procesy*, čestní generálové a poručíci, jsou *bezporuchové procesy*. Rozkaz útok, nebo ústup je jednobitová *zpráva* s hodnotou 1, nebo 0.

Správné řešení zmíněného problému musí splňovat tři podmínky:

- Časovou ohraničenost – musí být zaručeno, že procesy nakonec *dospějí k rozhodnutí* ohledně hodnoty zprávy, kterou obdrželi.
- Shodu na společné hodnotě zprávy – všechny bezporuchové procesy se musí *shodnout* na stejné hodnotě zprávy, kterou obdrželi.
- Platnost hodnoty, na které se procesy shodly – jestliže zpráva pochází od bezporuchového zdrojového procesu, musí se všechny ostatní bezporuchové procesy shodnout na stejné hodnotě, jakou vyslal zdrojový proces.

Zajímavým vedlejším efektem splnění těchto podmínek je, že i přesto že je zdrojový proces poruchový, musí se ostatní bezporuchové procesy shodnout na stejné hodnotě zprávy. Je jedno, jestli se shodnou na hodnotě 0, nebo 1, ale musí se shodnout. Takže i když poruchový zdrojový proces předá

každému bezporuchovému procesu jinou hodnotu, bezporuchové procesy se stejně musí shodnout na jedné společné hodnotě.

Existují dva algoritmy řešící zmíněný problém:

- Oral Messages OM
- Signed Messages SM

Algoritmus OM je schopen zajistit splnění podmínek za předpokladu, že bezchybných procesu je více než trojnásobek chybných procesů. Tzn. pro jeden chybný proces potř. další 3 bezchybné. Druhý algoritmus předpokládá, že všechny bezchybné procesy jsou schopné poznat pečeť bezchybného zdrojového procesu. Pečeť zprávy od bezchybného zdrojového procesu nemůže být ani zfalšována chybným procesem, jinými slovy bezchybné procesy poznají snahu o změnění zprávy pocházející od bezchybného zdrojového procesu. Tento algoritmus je schopen splnit podmínky i pro 3 procesy, z nichž jeden je chybný. Principy obou algoritmů je možno najít v pramenech [Fault16 a Fault18].

3. Realizace

Všechny dosud uvedené informace slouží jako podklad pro vlastní návrh jištěného řídicího systému MVE. Jeho klíčové vlastnosti zahrnují:

- Schopnost obsluhovat 1 – 10 turbín.
- Zajištění podmínek pro bezpečný provoz soustrojí turbína-generátor.
- Regulaci otevření turbín podle množství vody v řece.
- Trojnásobná záloha řídicího systému.

K dosažení tohoto cíle, byl zvolen následující postup:

- Navržení nezálohovaného řídicího systému MVE, na němž bude ověřena schopnost zajistit bezpečný provoz a regulaci turbín MVE.
- Navržení úprav nezálohovaného řídicího systému, tak aby byl trojnásobně zálohovaný.
- Realizace zálohovaného (jištěného) systému a ověření funkčnosti navržených mechanismů zajištění.

3.1 Nezálohovaný řídicí systém MVE

Zajištění bezpečného provozu soustrojí turbína-generátor znamená splnění podmínek uvedených v kapitole 1.4.1 Bezpečný chod soustrojí, pro připomenutí jsou zde uvedeny:

- Turbína (tím pádem i generátor) se nikdy nedostane do nebezpečně vysokých otáček
- Generátor není přetížen – proudy všech fází ani teplota nepřekročí povolenou velikost
- Všechny fáze sítě mají správné napětí
- Všechny fáze sítě mají správnou frekvenci
- Proudy fází jsou souměrné – žádná z fází není přetížena, ani přerušena
- Hladina na koruně jezu nikdy neklesne pod minimální úroveň
- Velikost napětí, pořadí (souslednost) fází a frekvence vyráběného napětí je v okamžiku sfázování shodná se sítí (synchronní generátor)
- Vyráběné napětí se nikdy nedostane do rozvodné sítě, není-li to bezpečné (pro synchronní generátor)

Systém, který je tyto podmínky schopen dodržet je principiálně možno realizovat několika způsoby:

- PLC automatem viz např. [Real1, Wiki3].
- Jedno-deskovým průmyslovým počítačem viz např. [Real2].
- Speciálně navrženým systémem s jednočipovým mikrokontrolérem (dále jen MCU).

Jednotlivá řešení mají různé výhody a nevýhody. Předností PLC automatu a Jedno-deskového průmyslového počítače je, že je pro ně potřeba vyvinout v podstatě jen programové vybavení. Vývoj systému, s jejich využitím, je tedy velmi rychlý. Je proto vhodný pro rychlé ověření navržených algoritmů. Hlavní nevýhodou ovšem je, že nelze zasahovat do technického

vybavení takového systému. Znamená to, že takový systém nelze modifikovat pro dosažení odolnosti proti poruchám.

Naproti tomu speciálně navržený systém je daleko složitější na realizaci, protože je potřeba navrhnout jak technické vybavení (hardware), tak i programové vybavení (software). Vložené úsilí se však vrátí, jelikož systém bude přesně splňovat zadání s největší efektivitou. Navíc bude připraven k úpravám, pro dosažení trojnásobného zálohování.

Pro realizaci řídicího systému MVE byla zvolena varianta speciálně navrženého systému s jednočipovým MCU.

3.2 Návrh a realizace nezálohovaného řídicího systému MVE

Návrh nezálohovaného řídicího systému MVE obnáší:

- Návrh blokové struktury řídicího systému.
- Výběr vhodného MCU a ostatních součástek.
- Návrh schématu řídicího systému na úrovni součástek.
- Návrh programového vybavení.
- Návrh způsobu ověření funkčnosti řídicího systému.

Ačkoli by se mohlo zdát, že jednotlivé kroky návrhu následují chronologicky jeden po druhém, není tomu tak. Např. výběr způsobu ověření funkčnosti řídicího systému ovlivní jeho blokovou strukturu. MCU je vybírán podle toho, jaký způsob připojení k PC a jaká sběrnice byla zvolena apod.

3.2.1 Výběr součástek

Při návrhu bylo nejdůležitější vybrat správný MCU. Požadavky na něj byly rozmanité, zde jsou některé z nich:

- Dostatečný výpočetní výkon.
- Podpora vybraných komunikačních protokolů (CAN, USB, I^2C).
- Dostupné vývojové a ladicí prostředky (kompilátor, vývojové prostředí, programátor/debugger).
- Dostupnost samotného MCU.
- Přijatelná cena.

V úvahu připadaly 8-bitové MCU AVR, firmy Atmel a PIC firmy Microchip. Tyto MCU ale nesplňovaly podmínku hardwarové podpory vybraných komunikačních protokolů a pokud už vybrané protokoly podporovaly, byly příliš drahé a těžko dostupné. Otázkou také bylo, jestli poskytnou dostatečný výpočetní výkon. Jako ideální se později ukázaly 32-bitové MCU s jádrem Cortex™-M3 vyvinutým firmou ARM. Poskytují vysoký výpočetní výkon, jejich pracovní frekvence se pohybuje okolo 50 – 100 MHz. Díky tomu je možné je provozovat i s *real time operačním systémem* (*RTOS*). Oplývají velkým množstvím hardwarově implementovaných periferií, mezi nimiž jsou i požadované CAN, USB a I^2C. Jejich spotřeba přitom nepřesahuje *150 mA*. Tyto MCU vyrábějí přední světoví výrobci jako Texas Instruments, STMicroelectronic, nebo NXP Semiconductors. Vývojové

prostředí k nim lze získat zdarma. Programátor/debugger je možné koupit za přijatelnou cenu okolo 1 500,- Kč. Jako úplně nejvhodnější se jevil MCU firmy Texas Intruments řady TMS570LS. Je postaven na dvou jádrech ARM Cortex™-R4F pracujících paralelně v režimu Lockstep. Tento procesor je však pro běžné zájemce těžko dostupný, vzorky stojí okolo $50, a není podporován bezplatnými vývojovými prostředími.

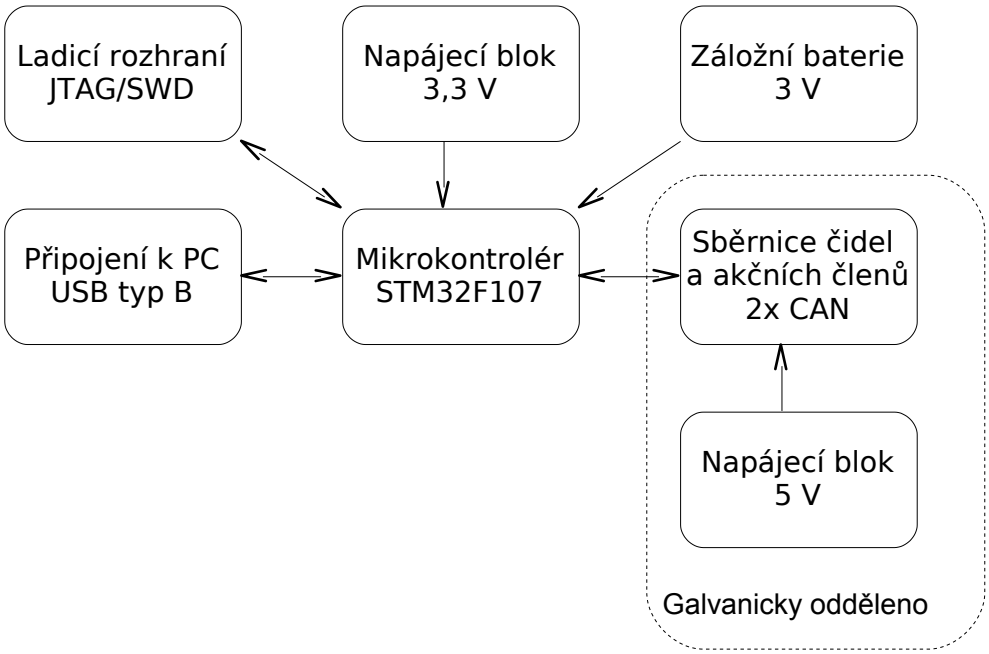
Proto byl nakonec vybrán procesor firmy STMicroelectronics řady STM32F107. Jeho hlavní parametry jsou:

- Jádro:
  - ARM 32-bit Cortex™-M3.
  - Maximální pracovní frekvence 72 MHz.
  - Výkon 1,25 DMIPS/MHz (Dhrystone 2.1), platí pro přístup do paměti s 0 čekacími stavy
  - Násobení a hardwarové dělení během jednoho hodinového cyklu
- Paměti:
  - 64 až 256 kB Flash,
  - až 64 kB volně přístupné SRAM
- Hodinový signál, reset a správa napájení
  - Napájecí napětí a napětí na portech 2,0 až 3,6 V
  - Reset po připojení napájení POR, reset po poklesu napájecího napětí pod danou mez PDR, programovatelný obvod hlídající napětí PVD (při poklesu pod danou mez, vyvolá přerušení)
  - Zdroj hodin může být krystal 3 až 25 MHz
  - Vnitřní RC oscilátor 8 MHz, trimovaný při výrobě
  - Vnitřní RC oscilátor 40 kHz s kalibrací
  - Možnost připojit oscilátor 32 kHz pro hodiny reálného času RTC
- Nízko-příkonové režimy
  - Režimy Sleep, Stop a Standby
  - Bateriové napájení VBAT pro RTC a záložní registry
- Dva 12-bitové, 1 µs A/D převodníky s 16 vstupy
  - Rozsah vstupního napětí: od 0 do 3,6 V
  - Schopnost provádět funkci S/H
  - Teplotní čidlo
  - V prokládaném režimu četnost převodu až 2 Ms/s
- Dva 12-bitové D/A převodníky
- DMA: 12-kanálový DMA řadič
- Implementované periferie: časovače, A/D převodníky, D/A převodíky, I^2S, SPI, I^2C a USART linky
- Debugovací režim
  - Sériové debugovací rozhraní SWD a rozhraní JTAG
  - Vestavěný trasovací blok Cortex-M3 Embedded Trace Macrocell™
- Maximálně 80 rychlých I/O pinů
  - 80 I/O pinů, které lze mapovat k 16 vektorům vnějšího přerušení

    - Téměř všechny I/O piny snesou 5 V
- Jednotka pro výpočet kontrolního součtu CRC, 96-bitové unikátní ID
- Maximálně 10 časovačů, jenž je možné mapovat k různým I/O pinům
- Maximálně čtyři 16-bitové časovače, každý až se 4 IC/OC/PWM nebo čítačem impulzů a vstupem kvadraturního inkrementujícího rotačního kodéru (quadrature incremental encoder)
- Jeden 16-bitový časovač, pro PWM řízení motorů, který umí generovat dead-time impulzy a má funkci nouzového zastavení
- Dva watchdog čítače jeden běžící nezávisle na systému a jeden s definovaným časovým oknem
- SysTick časovač: 24-bitový čítač směrem dolů, vhodný ke generování synchronizace pro RTOS
- Dva obyčejné 16-bitové čítače pro ovládání D/A převodníku
- Maximálně 14 komunikačních rozhraní, které je možno mapovat na různé I/O piny
- Maximálně dvě I^2C rozhraní podporující protokol SMBus/PMBus
- Maximálně 5 USART linek (ISO 7816 interface, LIN, IrDA a řízení modemu)
- Maximálně 3 SPI linky (18 Mbit/s), 2 přepínané s I2S rozhraním, které splňuje přesnost vyžadovanou audio aplikacemi
- Dvě CAN rozhraní (2.0B Active) s 512 B vyhrazené SRAM
- USB 2.0 full-speed řadič s režimy: device/host/OTG, PHY vrstva implementovaná na čipu, podporuje HNP/SRP/ID je pro něj vyhrazeno 1,25 kB paměti SRAM
- 10/100 Ethernet MAC s vyhrazeným DMA kanálem a 4 kB SRAM, podporuje hardware standardu IEEE1588 a MII/RMII

3.2.2 Návrh struktury nezálohovaného řídicího systému

Blokové schéma nezálohovaného řídicího systému MVE, je na obr. 5.



Obr. 5 Blokové schéma nezálohovaného řídicího systému

Řídicí systém se skládá z:

- Dvou oddělených napájecích částí
- Výpočetní části – MCU STM32F107
- Bloku komunikace s PC – USB portem typu B
- Bloku komunikace se sběrnicí s čidly a akčními členy – dvě sběrnice CAN

Systém je koncipován tak, že veškerá komunikace s vybavením řízené MVE probíhá po sběrnici CAN. Jsou na ni připojena všechna čidla podávající informace o stavu MVE i akční členy, které zajišťují její řízení. Pro každou turbínu jsou instalovány tato čidla:

- Velikostí otevření turbíny.
- Indikce úplného otevření/zavření turbíny – koncové spínače.
- Otáček turbíny.
- Otáček generátoru.
- Ampérmetry ve všech 3 fázích výstupu generátoru.
- Otáček generátoru.
- Teploty generátoru.

Navíc ještě mohou být instalována čidla:

- Teploty ložisek turbíny.
- Teploty ložisek generátoru.

Pro celou MVE jsou instalována čidla:

- Voltmetry ve všech 3 fázích přípojného místa MVE.
- Hladiny vody před česly.
- Hladiny vody za česly.
- Indikace menší hladiny na koruně jezu, než je minimální dovolená hodnota.
- Čítač frekvence síťového napětí.
- Hladiny vody u výtoku z MVE.

Pro každou turbínu jsou instalovány tyto akční členy:

- Servomotor ovládání otevření turbíny.
- Ovládání výkonového spínače, připojujícího generátor k rozvodné síti.
- Pro celou MVE, jsou instalovány tyto akční členy:
- Spínač automatického systému čištění česlí.
- Ovládání odpojovače celé silové části MVE.

MCU řídicího systému je napájen ze zdroje odděleného od zdroje pro napájení budičů sběrnice CAN. Oddělené napájení má dva důvody. Zaprvé, je procesor potřeba napájet napětím 3,3 V a budiče CAN sběrnice napětím 5 V. Zadruhé jsou použity speciální budiče CAN od firmy Texas Instruments, typ ISO 1050, s galvanickým oddělením. CAN sběrnice tedy není nijak elektricky spojena s MCU. To je velmi výhodné, protože CAN sběrnice prochází celou MVE a hrozí jí tedy potenciální riziko poškození, nemůže to ohrozit MCU.

Součástí řídicího systému jsou ještě součástky zajišťující chod MCU a konfiguraci, ze které paměti bude načítat program. Dále rozhraní SWD/JTAG pro programování a debugování MCU.

Schéma zapojení nezálohovaného řídicího systému je v příloze A. Výkres horní a dolní strany desky plošného spoje je v příloze B a příloze C.

3.2.3 Testování funkčnosti nezálohovaného řídicího systému

Je zřejmé, že testování řídicího systému přímo v MVE by bylo krajně nepraktické. Zaprvé by bylo potřeba navrhnout a vyrobit všechna čidla i akční členy, což je velice složité a nákladné. Zadruhé samotné testování řídicího systému v MVE je nevhodné.

Řídicí systém je tedy vybaven rozhraním USB, přes které je připojen k PC. Na PC běží program simulující chování MVE a vody v řece. Testování probíhá tak, že program na PC posílá řídicímu systému informace o stavu MVE stejně, jakoby pocházely od skutečných čidel připojených přes sběrnici CAN. Řídicí systém informace vyhodnocuje a programu na PC posílá zpět příkazy stejné, jaké by posílal skutečným akčním členům. Rozdíl je pouze v tom, že data posílá přes USB a nikoliv přes sběrnici CAN. Program pro PC obsahuje model chování hladiny vody na koruně jezu v závislosti na otevření turbín.

Model počítající výšku hladiny na koruně jezu je velice jednoduchý, přesto však dostatečný pro testování regulačního algoritmu řídicího systému.

V programu je možné nastavit kolik turbín MVE má. Základem modelu jsou tyto pravidla:

- Průtok řekou při maximální hladině na koruně jezu je roven hltnosti všech turbín otevřených na 100 %.
- Průtok řekou při minimální dovolené hladině na koruně jezu je roven hltnosti všech turbín otevřených na 10 %.
- V programu je možné nastavit profil, jak se mění hladina vody na koruně jezu při zavřené MVE.
- Přechod mezi dvěma stavy hladiny je lineární s koeficientem, který je parametrem měnitelným v programu.

V programu je také možno nastavovat splnění či nesplnění všech ostatních podmínek bezpečného chodu MVE:

- Generátor má správné otáčky – pro každou turbínu.
- Turbína má správné otáčky – pro každou turbínu.
- Proudy všech fázi generátoru jsou shodné a nepřekračují maximální dovolenou hodnotu – pro každou turbínu.
- Teplota generátoru je pod maximální hodnotou – pro každou turbínu.
- Všechny fáze rozvodné sítě mají správné napětí.
- Frekvence napětí rozvodné sítě je správné.
- Hladina vody na koruně jezu je nad minimální úrovní.

Testování regulačního algoritmu řídicího systému MVE probíhá tak, že uživatel v programu na PC:

- Nastaví počet turbín, které MVE má.
- Nastaví profil hladiny vody, která by byla na koruně jezu při zavřené MVE.
- Nastaví splnění všech podmínek bezpečného chodu MVE.
- Spustí test.

Po spuštění testu se děje toto:

- Řídicí systém si od programu na PC vyžádá data ze všech čidel. Tím zároveň zjistí, kolik turbín MVE má.
- Jelikož jsou splněny všechny podmínky bezpečného provozu MVE i podmínka minimální hladiny vody na koruně jezu, vydá systém povel k otevření turbín. Velikost počátečního otevření turbín, se řídí výškou hladiny na koruně jezu. Např. pro maximální výšku hladiny, vydá řídicí systém povel k otevření turbín na 80 %.
- Systém periodicky žádá o data z čidel až do chvíle, kdy přestane klesat výška hladiny vody na koruně jezu. Tzn., že program na PC dokončil modelování lineárního poklesu hladiny z hodnoty při zavřené MVE na hodnotu odpovídající aktuální velikosti otevření turbín.
- Řídicí systém porovná aktuální výšku hladiny vody na koruně jezu s minimální dovolenou výškou. Pokud je aktuální výška větší než minimální o více jak 10 %, vydá systém pokyn k otevření turbín o dalších 5 %.

- Takto řídicí systém čeká na zastavení poklesu hladiny a porovnává aktuální hladinu s minimální, až dosáhne stavu, kdy je aktuální hladina rovna minimální dovolené hladině + 5 %.
- V tomto stavu řídicí systém setrvá až do doby, kdy program na PC provede změnu hladiny na koruně jezu, podle profilu nastaveného na počátku uživatelem.
- Řídicí systém opět otevíráním, nebo zavíráním turbín dosáhne aktuálního stavu hladiny na koruně jezu rovného minimální dovolené hladině + 5 %.

Dále je možno testovat správnou reakci řídicího systému na nesplnění některé z podmínek bezpečného provozu MVE:

- Přehřátí, překročení maximálního proudu, překročení maximálních otáček, nebo nesouměrnost proudů ve fázích generátoru musí způsobit zavření příslušné turbíny a odpojení generátoru.
- Výpadek síťového napětí, nesprávná frekvence síťového napětí, nebo pokles hladiny vody na koruně jezu pod minimální dovolenou hodnotu musí způsobit zavření všech turbín a odpojení všech generátorů.

Řídicí systém by měl dále respektovat charakteristiku účinnosti turbíny, takže pokud má k dispozici více turbín a hladina vody na koruně jezu je malá, systém se bude snažit provozovat několik turbín blízko 80 % otevření. Ostatní turbíny zavře, protože tak dosáhne vyšší účinnosti využití průtoku vody dostupné v řece. Když už je hladina vody tak nízká, že nestačí ani na zásobování jediné turbíny otevřené alespoň okolo 50 %, přejde řídicí systém do pulzního režimu:

- Úplně zavře turbínu a počká, až hladina vody na koruně jezu stoupne.
- Turbínu otevře více, než dovoluje přítok řekou a nechá ji pracovat s vyšší efektivitou.
- Když hladina na koruně jezu opět klesne blízko minimální dovolené hodnoty, proces se opakuje.

Z dosud uvedeného by se mohlo zdát, že budiče sběrnice CAN jsou na nezálohovaném řídicím systému instalovány zbytečně. Není tomu tak. Ve druhé fázi realizace, kdy bude potřeba testovat řídicí systém vybavený trojnásobnou zálohou, bude nezálohovaný řídicí systém použit jako převodník USB/CAN. Trojnásobně zálohovaný systém bude opět testován pomocí programu na PC, simulujícího chování MVE a řeky, ale pro větší věrnost modelu budou data z PC přeposílána nezálohovaným řídicím systémem na sběrnici CAN. Pro trojnásobně zálohovaný systém se tedy bude situace jevit, jako by byl opravdu instalován v MVE a komunikoval se skutečnými čidly a akčními členy připojenými ke sběrnici CAN.

3.3 Návrh a realizace trojnásobně zálohovaného řídicího systému MVE

Předmětem této kapitoly je popis zodolnění nezálohované verze řídicího systému tak, aby byl trojnásobně zálohovaný. V tomto případě jde o vcelku jednoduchý krok. Srdcem celého řídicího systému je totiž MCU STM32F107 doplněný potřebnými obvody pro zajištění jeho funkce. Je tedy potřeba přidat další dva MCU a zajistit, aby dohromady tvořily systém TMR popsaný v kap. 2.4.2 Záloha typu TMR. Jelikož je jádro MCU dostatečně výkonné, bylo rozhodnuto, že vyhodnocování shody jednotlivých MCU bude provedeno na programové úrovni. Trojnásobně zálohovaný systém tedy bude obsahovat prvky SIFT popsané v kap. 2.4.3 Systém SIFT.

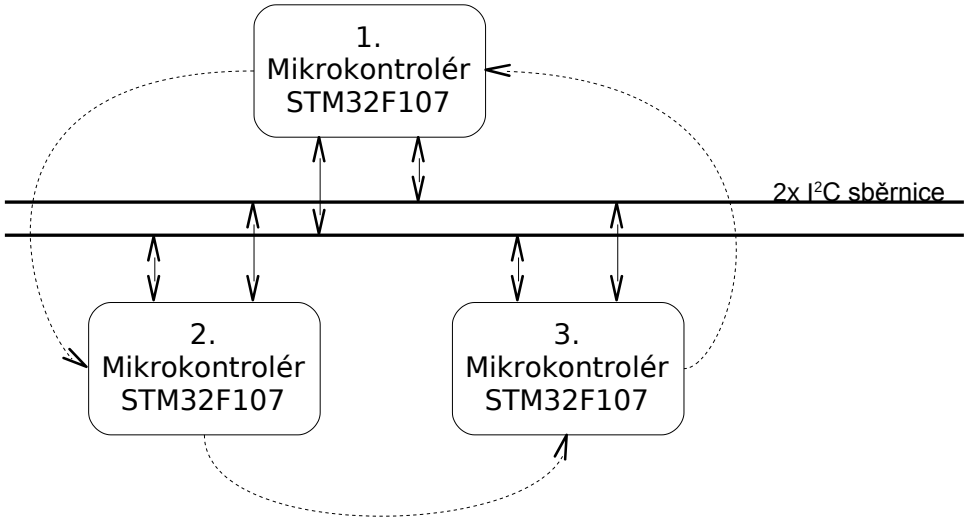
3.3.1 Programová implementace majoritního hlasovacího bloku

Toto řešení přináší výhodu veliké flexibility programového vybavení. Kdyby totiž bylo majoritní hlasování realizováno technickými prostředky (hardwarově), bylo by možné porovnávat jen jistý konkrétní formát výsledků dílčích MCU. Majoritní hlasovací blok je totiž omezen požadavkem na jeho velkou jednoduchost a z ní plynoucí řádově vyšší pravděpodobnost bezporuchového provozu, než mají použité MCU. Teoreticky je možné použít jako hlasovací blok další MCU, který je možno naprogramovat k porovnávání libovolných výsledků dodaných výpočetními MCU. Rozhodovací MCU je ale v takovém případě blokem s největší pravděpodobností selhání. Za přijatelně jednoduché a spolehlivé lze považovat programovatelné logické obvody GAL, SPLD, nebo maximálně CPLD.

Programově implementovaný majoritní rozhodovací blok SIFT ale přináší také nevýhody a problémy. Proces vedoucí k tomu, že se všechny tři MCU shodnou na *stejné* a *správné* hodnotě výsledku je poměrně komplikovaný. Více je tento problém rozebrán v kap. 2.4.3 Systém SIFT.

Pro účely testování jištěného řídicího systému MVE byl proto navržen jednodušší způsob majoritního hlasování o správnosti mezivýsledků zvaný Pešek. Není tak robustní a pro praktické použití jištěného řídicího systému by měl být nahrazen algoritmem SM z kap. 2.4.3 Systém SIFT. Implementace algoritmu SM je však náročná a proto byl pro ověřovací fázi vynechán.

Základem algoritmu Pešek je propojení všech tří MCU pomocí hlavní a záložní sběrnice I^2C viz obr. 6. MCU tvoří volně vázaný systém, který se synchronizuje a hlasuje o shodě před každým vysláním příkazu pro akční členy na sběrnici CAN. MCU se ve funkci řízení synchronizace a hlasování o příkazu, který bude vyslán na sběrnici CAN, periodicky střídají. Proces řídí vždy ten MCU, kterému byla přidělena funkce peška.



Obr. 6 Schéma činnosti algoritmu Pešek

Funkce systému v bezporuchovém stavu je následující:

- První MCU předá funkci peška druhému, zároveň o tom informuje i třetí MCU, který spustí odpočet časového limitu, do kterého mu druhý MCU musí předat funkci peška.
- Bezprostředně po té, co druhý MCU přijme funkci peška, si vyžádá data ze všech čidel a tomu samému vyzve i první a třetí MCU.
- Když druhý MCU, pešek, provede výpočet a má připraven k vyslání příkaz pro akční členy, dotáže se i prvního a třetího na jejich příkaz, ke kterému došli. Na základě obdržených výsledků vybere příkaz, který se objevil třikrát, nebo aspoň dvakrát a vyšle jej na sběrnici CAN. Poté předá funkci peška třetímu MCU a informuje o této skutečnosti první MCU – jeden cyklus skončil a začíná další.

Pokud se při porovnávání shodovaly jen příkazy od dvou MCU, je MCU, který dodal správnou hodnotu informován, že zbývající MCU provedl chybný výpočet. Tím je MCU s chybnou hodnotou vyřazen a navenek je indikována porucha. Porovnávání pak již probíhá jen mezi zbývajícíma dvěma MCU.

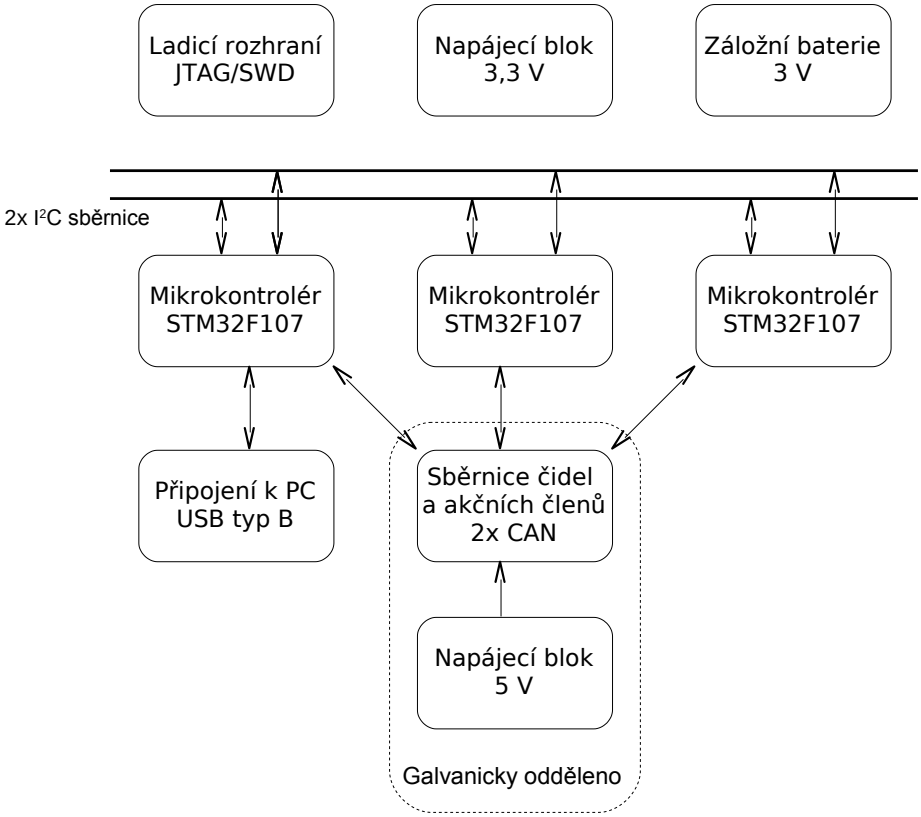
Celou proceduru od chvíle, kdy je MCU předána funkce peška, až po okamžik kdy má vyslat příkaz na sběrnici CAN a předat řízení

následujícímu MCU, musí MCU provést do časového limitu. Pokud MCU do vypršení časového limitu nepředá peška následujícímu MCU, je mu pešek následujícím MCU odebrán. Následující MCU se pokusí s předchozím, kterému byl odebrán pešek komunikovat. Pokud se to nepodaří, je vyřazen z rozhodování a navenek je signalizována jeho porucha.

Algoritmus Pešek je schopen odhalit chybný výpočet MCU, které zrovna nemají funkci peška. Je také schopen odhalit úplné zastavení kteréhokoliv MCU, i toho, který má funkci peška. Není však schopen odhalit chybný výpočet MCU, který je zrovna peškem. Samotné střídání funkce peška je způsobem jak potlačit tuto hlavní slabinu algoritmu Pešek.

3.3.2 Návrh struktury trojnásobně jištěného řídicího systému

Trojnásobně zálohovaná varianta řídicího systému striktně vychází z nezálohované varianty. Blokové schéma zálohovaného systému je na obr. 7. Proti nezálohované variantě přibyly dva MCU a dvě sběrnice I^2C zajišťující jejich vzájemnou komunikaci. Jedna je pracovní a druhá záložní. Pokud se jednomu MCU nepodaří kontaktovat ostatní MCU přes pracovní



Obr. 7 Trojnásobně zálohovaný řídicí systém

sběrnici, snaží se navázat spojení přes záložní sběrnici. Celá část s budiči sběrnice CAN je od zbytku řídicího systému galvanicky oddělena stejně jako u nezálohované varianty. Dvě sběrnice CAN mohou být využívány

stejným způsobem, jako sběrnice I^2C, tedy jedna jako pracovní a druhá jako záložní. Jinou možností je připojit ke každé z nich jinou sadu čidel a akčních členů. Takováto záloha čidla a akčních členů je však velice nákladná a proto musí být opodstatněná.

Blok napájení, záložní baterie a ladicí rozhraní jsou společné pro všechny tři MCU. Šipky znázorňující jejich připojení k jednotlivým MCU byly pro přehlednost vynechány. Schéma zapojení trojnásobně zálohovaného řídicího systému je v Příloze D. Výkres horní a dolní strany desky plošného spoje pak v příloze E a příloze F.

3.3.3 Testování funkčnosti trojnásobně zálohovaného řídicího systému

Probíhá obdobně jako u nezálohované varianty pomocí programu na PC simulujícího chování MVE a řeky. Připojení k PC se však nerealizuje přímo přes USB, ale prostřednictvím nezálohované varianty řídicího systému sloužícího jako převodník USB/CAN. I zálohovaná varianta řídicího systému je však vybavena USB konektorem, je připojen k prvnímu MCU. Může sloužit pro nouzové testování funkčnosti zálohovaného řídicího systému, nebo třeba pro upgrade jeho firmwaru ve finální verzi.

Zbytek procedury testování pak bude probíhat jako u nezálohované varianty řídicího systému z kap. 3.2.3.

3.3.4 Napájení trojnásobně zálohovaného řídicího systému

Napájecí zdroj pro zálohovaný řídicí systém nebyl součástí návrhu, předpokládá se však využití dvou síťových zdrojů zálohovaných akumulátory. Jeden z nich bude určen pro napájení všech MCU a druhy pro napájení budičů sběrnice CAN.

4. Závěr

Cílem práce bylo navrhnout a realizovat terciálně jištěný řídicí systém pro ovládání MVE s 1-10 turbínami. Zpětně lze konstatovat, že byla věnována příliš velká pozornost studiu teorie systémů odolných proti poruchám a zkoumání různých takových systému realizovaných ve světě. Odrazilo se to na samotném návrhu jištěného řídicího systému pro MVE. Zatímco hardware se podařilo dovést do fáze oživování modulů, software je zatím pouze slovně popsán. Práce na tomto projektu odhalila, jak rozsáhlou oblastí systémy odolné proti poruchám jsou.

Osobně mně byla práce přínosem hlavně díky nabytí poznatků z oblasti systémů odolných proti poruchám a rozšíření zkušeností o návrh obvodů s MCU ARM Cortex™-M3. Získal jsem také nové zkušenosti s návrhem desek plošných spojů.

Použitá literatura

[Elek0] ***Vodní elektrárny*** [online]. 25. 6. 2006 [cit. 2010-05-17]. Historie. Dostupné z WWW: <http://www.elektrarny.xf.cz/historie.php>.

[Elek1] ***Vodní a tepelné elektrárny*** [online]. -- [cit. 2010-05-16]. Vodní elektrárny v ČR. Dostupné z WWW: <http://www.vodni-tepelne-elektrarny.cz/vodni-elektrarny-cr.htm>.

[Elek2] ***Abeceda vodních pohonů*** [online]. -- [cit. 2010-05-17]. Historické mezníky. Dostupné z WWW: <http://mve.energetika.cz/uvod/stoleti.htm>.

[Elek3] ***Vodní elektrárny*** [online]. 25. 6. 2006 [cit. 2010-05-17]. Využití vodní energie + vodní elektrárny. Dostupné z WWW: <http://www.elektrarny.xf.cz/vyuziti.pdf>.

[Elek4] ***Abeceda vodních pohonů*** [online]. -- [cit. 2010-05-17]. O turbínách... Dostupné z WWW: <http://mve.energetika.cz/vodnimotory/turbiny-obecne.htm>.

[Elek5] ***SŠ prof. Zdeňka Matějčka*** [online]. -- [cit. 2010-05-18]. Generátory. Dostupné z WWW: <http://www.skolspec.cz/dokumenty/gilar/III.rocnik/generatory.pdf>.

[Elek6] ***VŠB TU Fakulta elektrotechniky a informatiky*** [online]. c2004 [cit. 2010-05-18]. Fázování synchronního generátoru k síti. Dostupné z WWW: <http://fei1.vsb.cz/kat453/www453/soubory/texty/ucebni_texty/se/cast_B_el_stroje/se_es_c2_fazovani.pdf>.

[Elek7] ***Abeceda vodních pohonů*** [online]. -- [cit. 2010-05-17]. Bánkiho turbína. Dostupné z WWW: <http://mve.energetika.cz/primotlaketurbiny/banki.htm>.

[Elek8] ***Vodní a tepelné elektrárny*** [online]. -- [cit. 2010-05-16]. Malé vodní elektrárny. Dostupné z WWW: <http://www.elektrarny.xf.cz/mve.php>.

[Elek9] ***Abeceda vodních pohonů*** [online]. -- [cit. 2010-05-23]. Časté chyby. Dostupné z WWW: <http://mve.energetika.cz/index.htm>.

[Fault1] KRINGS, Dr. Axel. ***Axel Krings Faculty Page : Fault-Tolerant Systems (CS449/549)*** [online]. 2009 [cit. 2010-05-23]. Lecture Notes, Lecture 1, Sequence 1. Dostupné z WWW: <http://www2.cs.uidaho.edu/~krings/CS449/Notes.F09/449-09-01.pdf>.

[Fault2] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Vydání první. Praha : Vydavatelství ČVUT, 1992. 330 s. ISBN 80-01-00852-5.

[Fault3] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 1.1 Definice spolehlivosti, s. 330. ISBN 80-01-00852-5.

[Fault4] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 1.2 Metody řízení spolehlivosti, s. 330. ISBN 80-01-00852-5.

[Fault5] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 1.2.1 Předcházení poruchám, s. 330. ISBN 80-01-00852-5.

[Fault6] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 1.1.1 Ukazatele spolehlivosti neobnovovaných objektů, s. 330. ISBN 80-01-00852-5.

[Fault7] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 1.1.2 Ukazatele spolehlivosti obnovovaných objektů, s. 330. ISBN 80-01-00852-5.

[Fault8] KRINGS, Dr. Axel. ***Axel Krings Faculty Page : Fault-Tolerant Systems (CS449/549)*** [online]. 2009 [cit. 2010-05-24]. Lecture Notes, Lecture 2, Sequence 2. Dostupné z WWW: <http://www2.cs.uidaho.edu/~krings/CS449/Notes.F09/449-09-02.pdf>.

[Fault9] KRINGS, Dr. Axel. ***Axel Krings Faculty Page : Fault-Tolerant Systems (CS449/549)*** [online]. 2009 [cit. 2010-05-24]. Lecture Notes, Lecture 6, Sequence 5. Dostupné z WWW: <http://www2.cs.uidaho.edu/~krings/CS449/Notes.F09/449-09-05.pdf>.

[Fault10] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 1.2.2 Odolnost proti poruchám, s. 330. ISBN 80-01-00852-5.

[Fault11] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 3 Zálohování, s. 330. ISBN 80-01-00852-5.

[Fault12] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 2.1.4 Modely využívající stavový graf, s. 330. ISBN 80-01-00852-5.

[Fault13] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 5.2.2 SIFT, s. 330. ISBN 80-01-00852-5.

[Fault14] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 6.3.2 Programové vybavení SIFT, s. 330. ISBN 80-01-00852-5.

[Fault15] KRINGS, Dr. Axel. ***Axel Krings Faculty Page : Fault-Tolerant Systems (CS449/549)*** [online]. 2009 [cit. 2010-05-23]. Lecture Notes, Lecture 1, Sequence 29. Dostupné z WWW: <http://www2.cs.uidaho.edu/~krings/CS449/Notes.F09/449-09-29.pdf>.

[Fault16] NELSON, Mark. ***Mark Nelson : Programming, mostly.*** [online]. 2007-07-23 [cit. 2010-05-26]. The Byzantine Generals Problem. Dostupné z WWW: <http://marknelson.us/2007/07/23/byzantine/>.

[Fault17] HLAVIČKA, Jan, et al. ***Číslicové systémy odolné proti poruchám.*** Praha : Vydavatelství ČVUT, 1992. 5.1.1 Počátky, s. 330. ISBN 80-01-00852-5.

[Fault18] WANG, Muyuan. ***The Byzantine General Problem.*** [online]. 2009 [cit. 2010-05-27]. Dostupné z WWW:

<http://ants.mju.ac.kr/2009Spring/ComputerSecurity/byzantine%20general%20summary.ppt>.

[Real1] ***Obsah dokumentace PROMOTIC*** [online]. [cit. 2010-05-26]. Seznam PLC automatů a komunikačních protokolů. Dostupné z WWW: <http://www.promotic.eu/cz/pmdoc/Subsystems/Comm/PLC/Group.htm>.

[Real2] ***IBSmm*** [online]. -- [cit. 2010-05-26]. IBSmm Products. Dostupné z WWW: <http://www.ibsmm.com/index1.php>.

[ObrElek1] ***Abeceda malých vodních pohonů*** [online]. -- [cit. 2010-05-18]. Vodní dílo jezové. Dostupné z WWW: <http://mve.energetika.cz/vodnidilo/voddilo-jezove.htm>.

[ObrElek2] ***Abeceda malých vodních pohonů*** [online]. -- [cit. 2010-05-18]. Vodní dílo derivační. Dostupné z WWW: <http://mve.energetika.cz/vodnidilo/voddilo-derivacni.htm>.

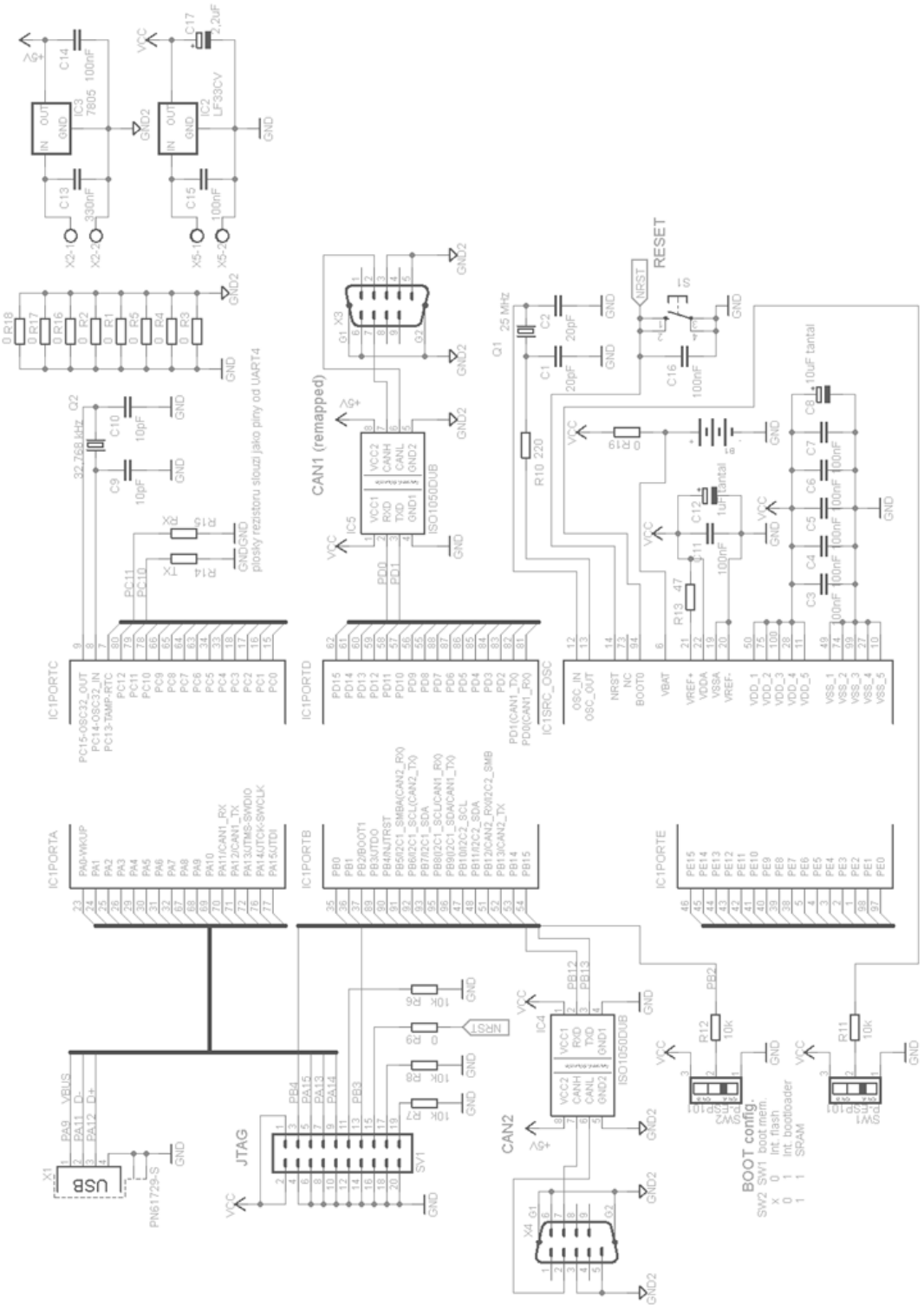
[Wiki1] ***Seznam vodních elektráren v Česku*** In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 16. 2. 2007, 16. 11. 2009 [cit. 2010-05-16]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Seznam_vodn%C3%ADch_elektr%C3%A1ren_v_%C4%8Cesku>.

[Wiki2] ***Malá vodní elektrárna*** In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 16. 2. 2007, 17. 12. 2009 [cit. 2010-05-17]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Mal%C3%A1_vodn%C3%AD_elektr%C3%A1rna>.

[Wiki3] ***Programovatelný logický automat*** In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 31. 10. 2006, 20. 5. 2010 [cit. 2010-05-26]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Programovateln%C3%BD_logick%C3%BD_automat>.

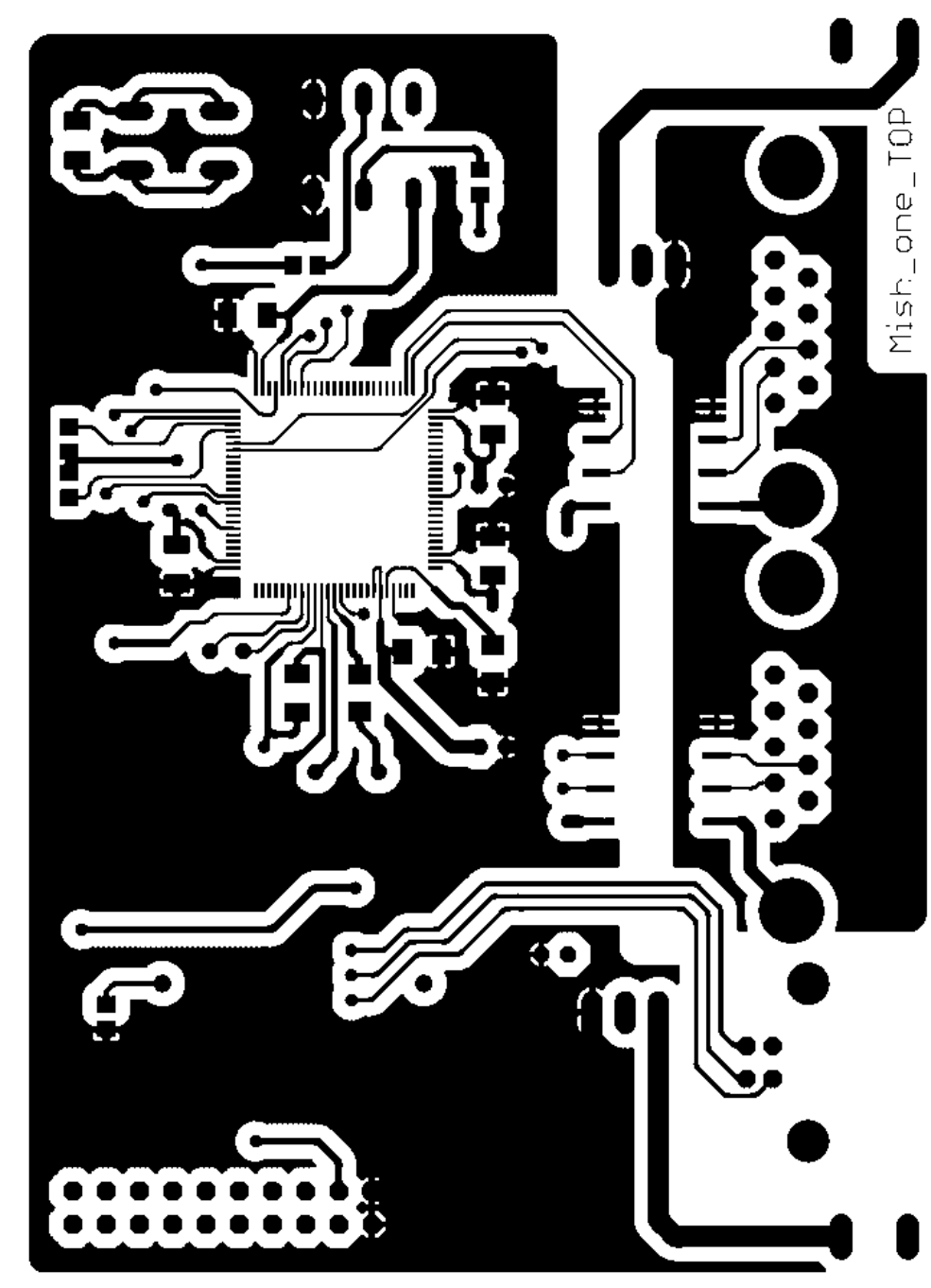
Příloha A

Schéma zapojení nezálohovaného řídicího systému.



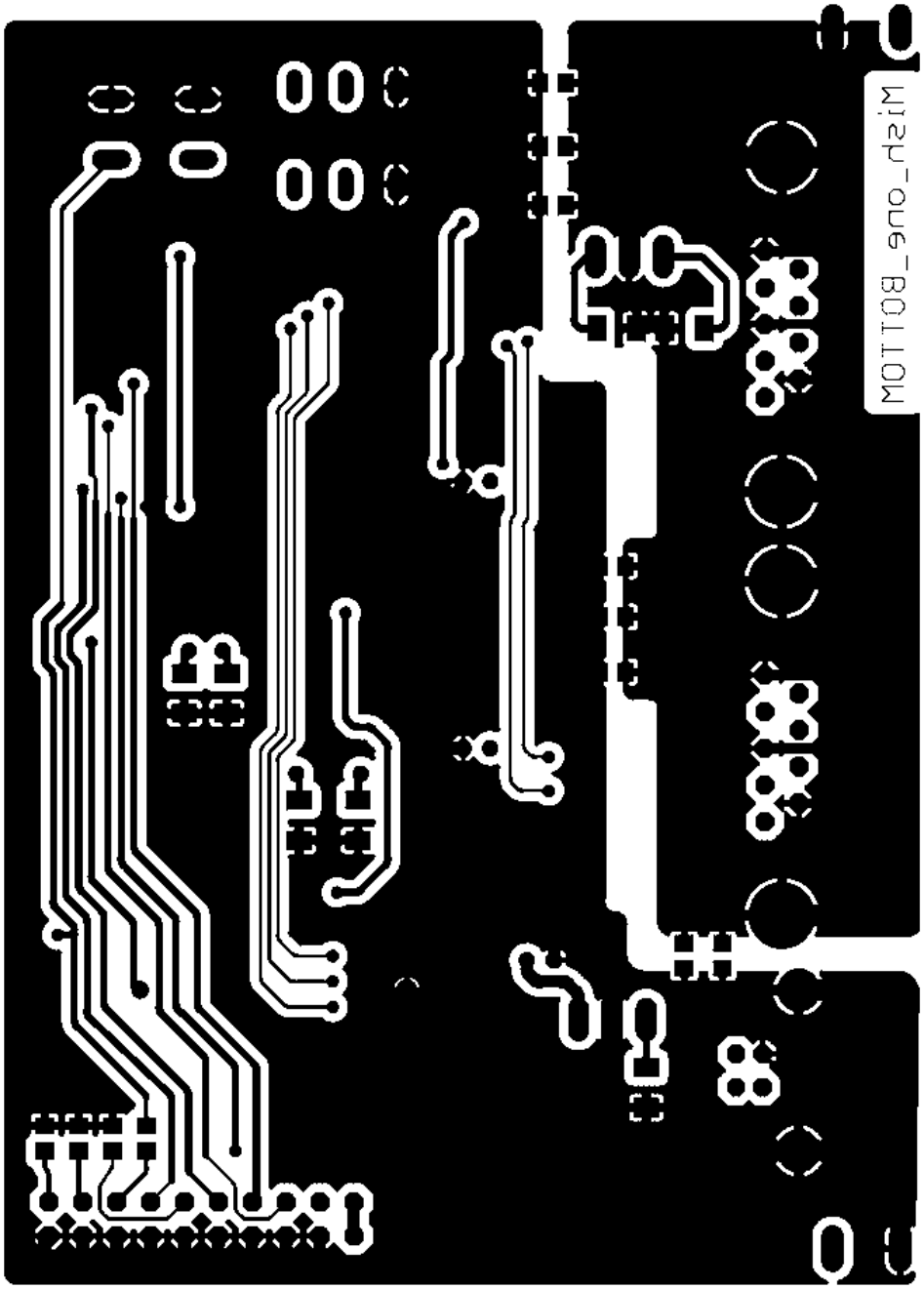
Příloha B

Motiv plošných spojů nezálohovaného řídicího systému, horní strana.



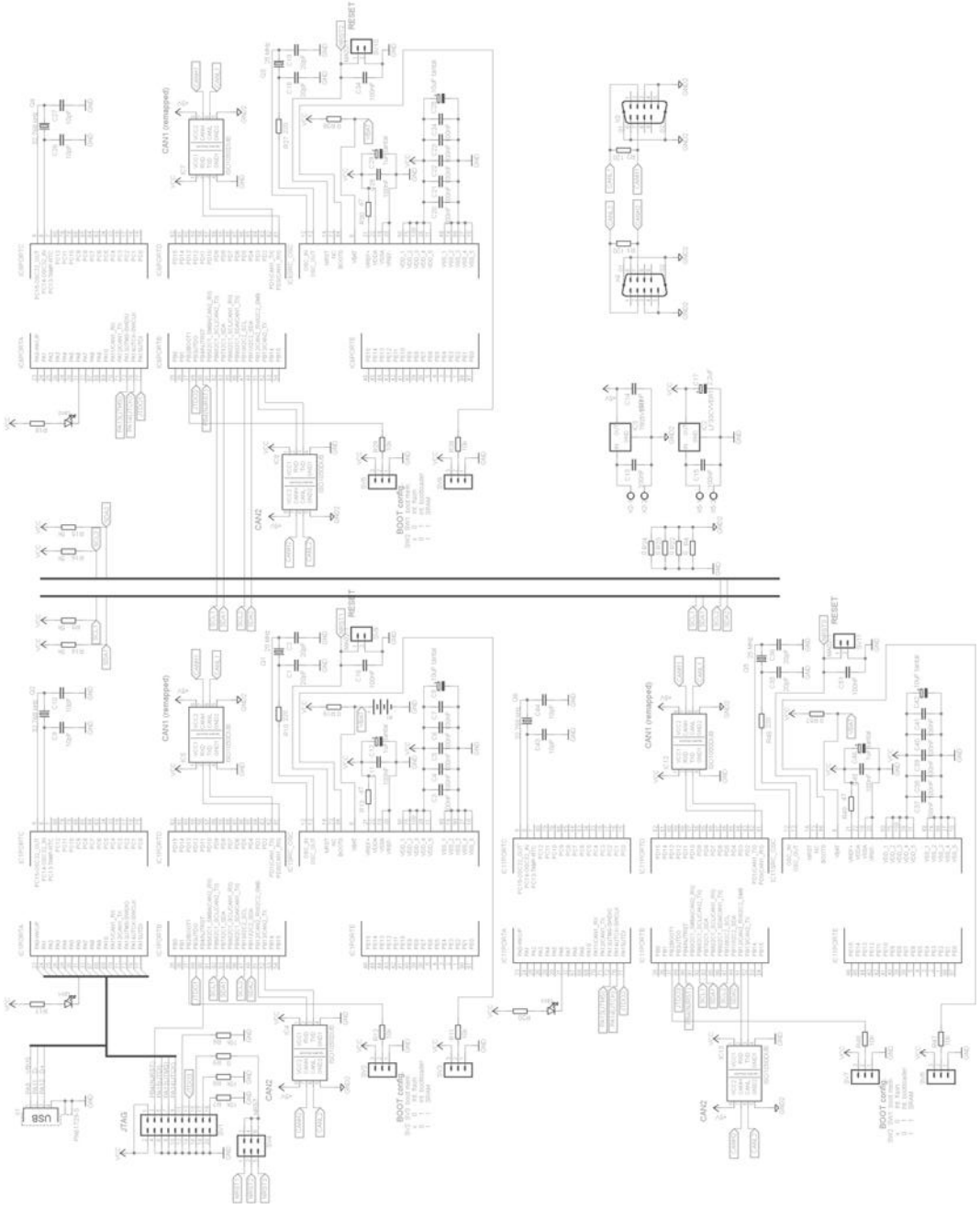
Příloha C

Motiv plošných spojů nezálohovaného řídicího systému, dolní strana.



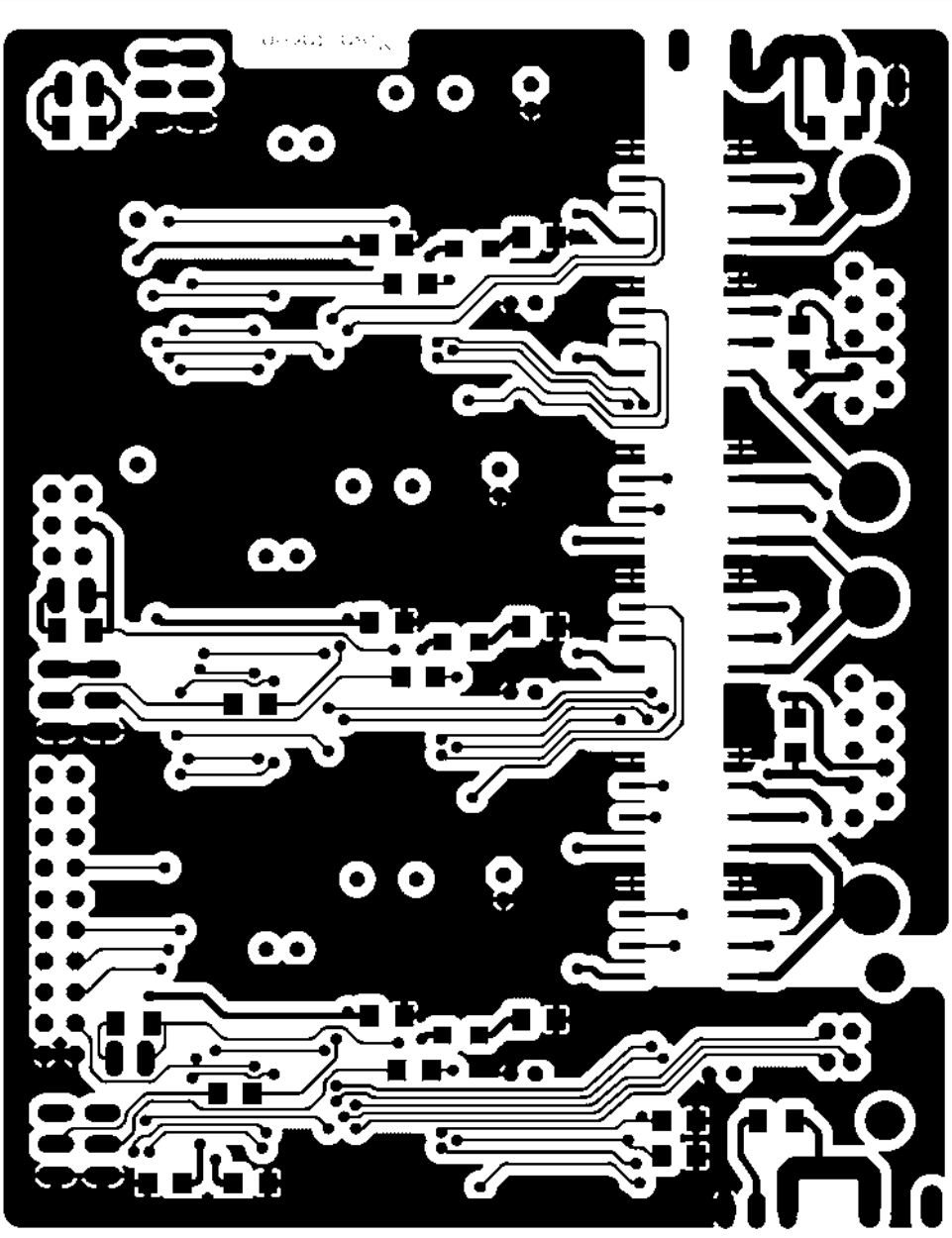
Příloha D

Schéma zapojení trojnásobně zálohovaného řídicího systému.



Příloha E

Motiv plošných spojů trojnásobně zálohovaného řídicího systému, horní strana.



Příloha F

Motiv plošných spojů trojnásobně zálohovaného řídicího systému, dolní strana.